

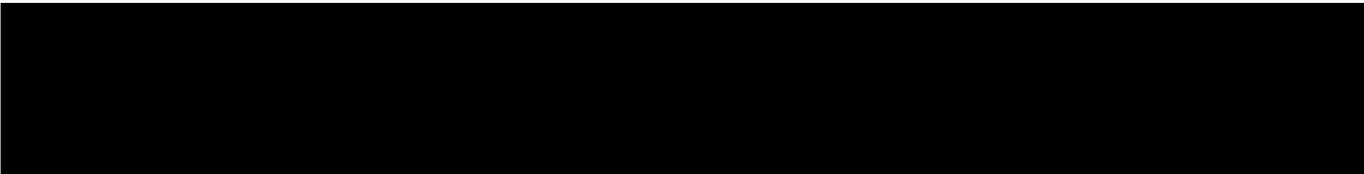
~~TOP SECRET//SI//NOFORN/FISA~~



(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: June 1, 2017– November 30, 2017

DECEMBER 2019



~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

**(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND
GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN
INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL
AND THE DIRECTOR OF NATIONAL INTELLIGENCE**

DECEMBER 2019

TABLE OF CONTENTS

(U) Executive Summary	5
(U) Section 1: Introduction	6
(U) Section 2: Oversight of the Implementation of Section 702	8
(U) I. Joint Oversight of NSA	9
(U) II. Joint Oversight of FBI	11
(U) III. Joint Oversight of CIA	14
(U) IV. Joint Oversight of NCTC	16
(U) V. Interagency/Programmatic Oversight	17
(U) VI. Training	18
(U) Section 3: Trends in Section 702 Targeting and Minimization	19
(U) I. Trends in NSA Targeting and Minimization	19
(U) II. Trends in FBI Targeting	24
(U) III. Trends in CIA Minimization	26
(U) IV. Trends in NCTC Minimization	29
(U) Section 4: Compliance Assessment – Findings	30
(U) I. Compliance Incidents – General	30
(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures	42
(U) III. Review of Compliance Incidents – FBI Targeting and Minimization Procedures	52
(U) IV. Review of Compliance Incidents – CIA Minimization Procedures	56
(U) V. Review of Compliance Incidents – NCTC Minimization Procedures	57
(U) VI. Review of Compliance Incidents – Provider Errors	57
(U) Section 5: Conclusion	58
(U) Appendix	A-1

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

(U) FACT SHEET

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Joint Assessments

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as “Joint Assessments,” and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of December 2019, nineteen Joint Assessments have been submitted.

(U) Joint Assessment Basics:

- (U) *Why is the Joint Assessment required?* The FISA Amendments Act of 2008 (50 U.S.C. § 1881a(l)(1)) requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702.
- (U) *What period is covered by a Joint Assessment?* Each Joint Assessment covers a six-month period: December 1 – May 31 or June 1 – November 30.
- (U) *Who receives it?* Each Joint Assessment is submitted to the following oversight entities: Foreign Intelligence Surveillance Court (FISC), relevant congressional committees, and the Privacy and Civil Liberties Oversight Board (PCLOB).
- (U) *What is being assessed?* The Attorney General and the DNI jointly assess the Government’s compliance with guidelines and FISC-approved “targeting” and “minimization” procedures and, in October 2018, “querying” procedures. The FISA Amendments Reauthorization Act of 2017 codified new requirements concerning Section 702, including requiring “querying” procedures.
- (U) *What are targeting, minimization, and querying procedures?* Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information. Querying procedures set rules for using United States person and non-United States person identifiers to query Section 702-acquired information. Prior to the FISA Amendments Reauthorization Act of 2017 codification, the minimization procedures contained querying rules. The 2018 certifications (which were outside this current assessment’s reporting period) were the first certifications to contain the newly required querying procedures.

(U) Highlights from 19th Joint Assessment:

- (U) *Compliance incident rate remains low.* The compliance incident rate remained low, which is consistent with the compliance incident rate reported for other reporting periods. The majority of incidents were caused by a misunderstanding of the procedures, failure to conduct the required checks, technical issues, and inadvertent human errors.
- (U) *Continued focused efforts to implement Section 702 in a compliant manner.* This Joint Assessment reports that the agencies continued to implement the procedures in a manner that reflects a focused and concerted effort by Intelligence Community (IC) personnel to comply with the requirements of Section 702.

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

- *(U) What compliance and oversight efforts underlie the Joint Assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, and constitutional requirements. A joint oversight team consisting of experts from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) oversee these measures. Each incident of non-compliance (*i.e.* compliance incident) is documented, reviewed by the joint oversight team, remediated, and reported to the FISC and relevant congressional committees. The Joint Assessment summarizes trends and assesses compliance (including calculating the compliance incident rate for the relevant reporting period) and may include recommendations to help prevent compliance incidents or increase transparency.
- *(U) What government agencies are involved with implementing Section 702?* The National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC). Each Joint Assessment discusses how these agencies implement the authority.
- *(U) Why is the Joint Assessment classified?* The Joint Assessment is classified to allow the Government to provide the FISC, congressional oversight committees, and the PCLOB a complete assessment of the Section 702 program, while at the same time protecting sources and methods. They are carefully redacted for public release in the interest of transparency.
- *(U) What is the format of the Joint Assessment?* The Joint Assessment generally contains an Executive Summary, five sections, and an Appendix. Beginning with the 16th Joint Assessment, this fact sheet has been included. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts, and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews of the targeting and minimization procedures. Section 4 describes compliance trends. The Joint Assessment describes the extensive measures undertaken by the Government to ensure compliance with court-approved targeting and minimization procedures; to accurately identify, record, and correct errors; to take responsive actions to remove any erroneously obtained data; and to minimize the chances that mistakes will re-occur.
- *(U) What are the types of compliance incidents discussed?* Generally, the Joint Assessment groups incidents into six or seven categories. Categories 1-4 (tasking incidents, detasking incidents, notification delays, and documentation errors) discuss non-compliance with targeting procedures. Category 5 discusses incidents of non-compliance with minimization procedures, such as erroneous queries of Section 702-acquired information using United States person identifiers. When appropriate, a category discussing incidents of overcollection is included. Additionally, the last category is a catch-all category for incidents that do not fall into one of the other categories. The actual number of the compliance incidents is classified; the percentage breakdown of those incidents is unclassified and reported in the Joint Assessment. Additionally, because Section 702 collection occurs with the assistance of U.S. electronic communications service providers who receive a Section 702(h) directive, the Joint Assessment includes a review of any compliance incidents by such service providers.

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence

December 2019

Reporting Period: June 1, 2017 through November 30, 2017

(U) EXECUTIVE SUMMARY

(U) The FISA Amendments Act of 2008 (hereinafter “FAA”) requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended (hereinafter “FISA” or “the Act”), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting and minimization procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the nineteenth joint compliance assessment of the Section 702 program. This assessment covers the period from June 1, 2017 through November 30, 2017 (hereinafter the “reporting period”) and accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act as required by Section 707(b)(1) of FISA (hereinafter “the Section 707 Report”). The Department of Justice (DOJ) submitted the Section 707 Report on March 5, 2018; it covers the same reporting period as the Joint Assessment.

(U) This Joint Assessment is based upon the compliance assessment activities that have been jointly conducted by the DOJ’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI).

(U) This Joint Assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities and to impose internal controls for compliance and verification purposes. The compliance incidents that occurred during this reporting period represent a very small percentage (0.42%) of the overall collection activity. However, as explained in past assessments and detailed later in this current assessment, the overall compliance incident rate is an imperfect metric; for example, the actual rate is determined by comparing dissimilar factors. To enhance overseers’ and the public’s understanding of Section 702 compliance, this current assessment includes a new metric: the targeting assessment compliance rate for the National Security Agency (NSA) (Figure 16).

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) SECTION 1: INTRODUCTION**

(U) The FISA Amendments Act of 2008 (hereinafter, “FAA”)¹ requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended (hereinafter, “FISA” or “the Act”), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice’s (DOJ) National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter, “Section 702”) have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI’s 19th joint compliance assessment under Section 702, covering the period June 1, 2017 through November 30, 2017 (hereinafter, the “reporting period”).²

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting and minimization procedures, as well as guidelines. A primary purpose of the guidelines is to ensure compliance with the limitations set forth in subsection (b) of Section 702, which are as follows:

An acquisition authorized under subsection (a)—

- (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

The Attorney General’s Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter “the Attorney

¹ (U) On January 18, 2018, Congress reauthorized FAA with the FISA Amendments Reauthorization Act of 2017, with an effective date of December 31, 2017; it codified new requirements concerning Section 702. However, because the Act was signed into law after this current joint assessment’s reporting period, any new requirements and how the government implements those requirements – including amended statutory citations – are not discussed in this joint assessment; they will be addressed in subsequent joint assessment(s), as appropriate.

² (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on March 5, 2018, as required by Section 707(b)(1) of FISA (hereafter Section 707 Report). This 19th Joint Assessment covers the same reporting period as the 19th Attorney General’s Section 707 Report.

~~TOP SECRET//SI//NOFORN/FISA~~

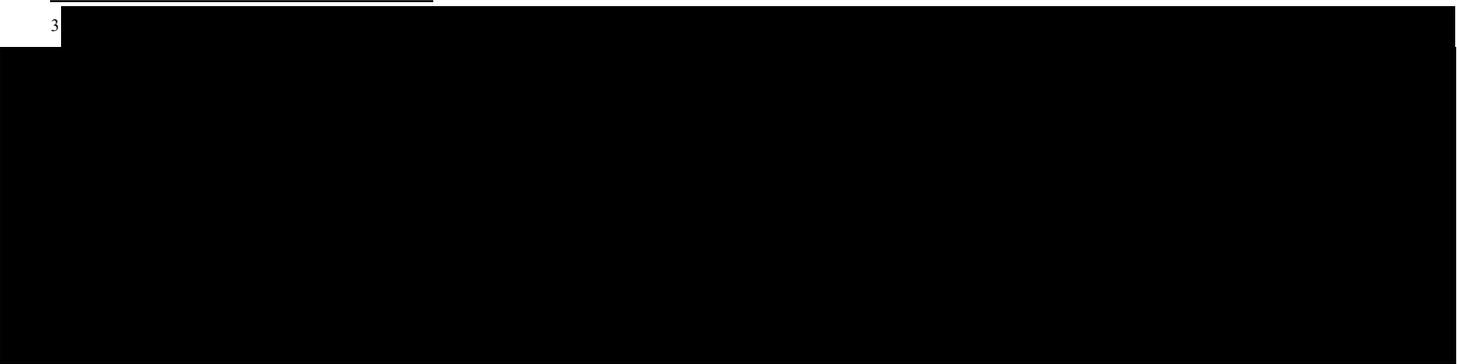
~~TOP SECRET//SI//NOFORN/FISA~~

General's Acquisition Guidelines") were adopted by the Attorney General, in consultation with the DNI, on August 5, 2008.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information.³ Four agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC).⁴ An overview of how these agencies implement the authority appears in the Appendix of this assessment.

(U) Section Two of this Joint Assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting and minimization procedures, as well as the Attorney General's Acquisition Guidelines. Section Three compiles and presents data acquired from the joint oversight team's compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the Section 707 Report. As with the prior Joint Assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent recurrences. Finally, this Joint Assessment contains an Appendix. The Appendix, also contained in previous joint assessments, details how each agency implements Section 702 and includes a general description of the oversight at each agency.

3



⁴ (U) As reported in the previous Joint Assessment, in an opinion issued by the FISC on April 26, 2017 (hereafter the FISC's April 2017 Opinion), the FISC authorized the NCTC to receive unminimized Section 702 data when it approved new minimization Section 702 procedures for NCTC (2016 NCTC Minimization Procedures). Both the FISC opinion and the 2016 NCTC Minimization Procedures were posted, in redacted form, on ODNI's website *IC on the Record* on May 11, 2017. The 2016 NCTC Minimization Procedures reflect that NCTC may receive unminimized Section 702 information. Prior to the approval of the 2016 NCTC Minimization Procedures, NCTC was not authorized to receive unminimized Section 702 information pertaining to counterterrorism. However, under both the prior minimization procedures and the current procedures, NCTC ingests data from FBI systems that contain minimized Section 702 information. Because NCTC is not a law enforcement agency, it may not receive disseminations of Section 702 information that contain evidence of a crime, but which have no foreign intelligence value.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) In summary, the joint oversight team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period. In its ongoing efforts to reduce the number of future compliance incidents, the Government will continue to focus on measures to improve (a) inter and intra-agency communication, (b) training, and (c) systems used in the handling of Section 702-acquired communications, including those systems needed to ensure that appropriate purge practices are followed and that certain disseminated reports are withdrawn as required. Further, the joint oversight team will also continue to monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report. Each joint assessment provides updates, as appropriate, on these on-going efforts.

(U) SECTION 2: OVERSIGHT OF THE IMPLEMENTATION OF SECTION 702

(U) The implementation of Section 702 is a multi-agency effort. As described in detail in Appendix A, NSA and FBI each acquire certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, CIA, and NCTC⁵ each handle Section 702-acquired data in accordance with their own minimization procedures.⁶ There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies from using preexisting systems to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

(U) A joint oversight team was established to conduct compliance assessment activities, consisting of members from NSD, the ODNI Office of Civil Liberties, Privacy, and Transparency (ODNI CLPT), the ODNI Office of General Counsel (ODNI OGC), and the ODNI Office of the Deputy Director for Intelligence Integration/Mission Integration Division (ODNI DD/II/MID). The team members play complementary roles in the review process. The following section, which has

⁵ (U) As discussed herein, CIA and NCTC receive Section 702-acquired data from NSA and FBI.

⁶ (U) Each agency's Section 702 targeting and minimization procedures, and with the codification of the FISA Amendments Reauthorization Act of 2017, querying procedures, are approved by the Attorney General and reviewed by the FISC. Because Attorney General approved querying procedures only became effective with the FISC-approved 2018 certifications, in October 2018, this current assessment does not assess compliance with those querying procedures as their application is outside the reporting period. However, query rules were contained in the minimization procedures and compliance with the query rules in the agencies' respective minimization procedures is assessed and discussed within this assessment.

(U) On May 11, 2017, the DNI released, in redacted form, the 2016 minimization procedures for NSA, FBI, CIA, and NCTC, as well the 2016 targeting procedures, in redacted form, for NSA and FBI. These procedures are posted on ODNI's *IC on the Record* website. While outside this assessment's reporting period, the procedures (including the newly required querying procedures) and the associated court opinions for the 2018 certifications were posted on *IC on the Record* on October 8, 2019.

~~TOP SECRET//SI//NOFORN/FISA~~

been reordered from previous assessments,⁷ describes the oversight activities of the joint oversight team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this Joint Assessment.

(U) I. Joint Oversight of NSA

(U) Under the process established by the Attorney General and Director of National Intelligence’s certifications, all Section 702 targeting is initiated pursuant to the NSA targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities⁸ (also referred to as selectors) once collection begins. NSA must also minimize its collection in accordance with its minimization procedures. Each of these responsibilities is detailed in the Appendix. Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities. NSA’s internal oversight and compliance mechanisms are further described in the Appendix.

(U) NSD and ODNI’s joint oversight of NSA’s implementation of Section 702 consists of periodic compliance reviews, which the NSA targeting procedures require,⁹ as well as the investigation and reporting of specific compliance incidents. During this reporting period, onsite reviews were conducted at NSA on the dates shown in Figure 1.

(U) Figure 1: NSA Reviews

UNCLASSIFIED

Date of NSA Onsite Review	Targeting and Minimization Reviewed
August 25, 2017	June 1, 2017 – July 31, 2017
October 27, 2017	August 31, 2017 – September 30, 2017
December 15, 2017	October 1, 2017 – November 30, 2017

(U) Figure 1 is UNCLASSIFIED.

(U) Reports for each of these reviews document the relevant time period of the review, the number and types of communication facilities tasked, and the types of information that NSA relied

⁷ (U) This section has been reordered from previous assessments that had started with describing the joint oversight of NSA, CIA, FBI, and NCTC. This current assessment now describes joint oversight of NSA, FBI, CIA, and NCTC. This revised order better aligns with the type of oversight conducted at each agency. Specifically, as explained herein, both NSA and FBI have targeting and minimization procedures, thus NSD and ODNI conduct both targeting and minimization reviews. Additionally, as explained herein, CIA and NCTC only have minimization procedures for which NSD and ODNI conduct reviews.

⁸ (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities (*i.e.* selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described in this joint assessment, applies to the targeting of every communication facility, regardless of the type of facility. A fuller description of the Section 702 targeting process may be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and is not attempting to make a substantive distinction between the two terms.

⁹ (U) The NSA targeting procedures require that the onsite reviews occur approximately every two months.

~~TOP SECRET//SI//NOFORN/FISA~~

upon, as well as provide a detailed summary of the findings for that reporting period. These reports have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

(U) The joint oversight review process for NSA targeting begins well before the onsite review. Prior to each onsite review, NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the reporting period to NSD and ODNI. Members of the joint oversight team initially review the tasking sheets, with ODNI team members sending any questions they may have concerning the tasking sheets to NSD, who then prepares a detailed report of the findings, including any questions and requests for additional information. NSD shares this report with the ODNI members of the joint oversight team. During this initial review, the joint oversight team determines whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information to ascertain the basis for NSA's foreignness determinations. The joint oversight team also reviews whether the tasking was in conformance with the targeting procedures and statutory requirements. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that did not provide sufficient information and requests additional information.

(U) During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets, together with the NSA Office of Compliance for Operations (OCO), NSA attorneys, and other NSA personnel, as required. The joint oversight team works with NSA to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of electronic and telephonic exchanges to answer questions and clarify issues.

(U) The joint oversight team also reviews NSA's minimization of Section 702-acquired data. NSD currently reviews all of the serialized reports (ODNI reviews a sample) that NSA has disseminated and identified as containing Section 702-acquired United States person information. The team also reviews a sample of serialized reports that NSA has disseminated and identified as containing Section-702 acquired *non*-United States person information. NSD and ODNI also review a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) NSA's Section 702 minimization procedures provide that any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures,¹⁰ which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information, as defined in FISA. With respect to queries of Section 702-acquired *content* using a United States person identifier, the joint oversight team reviews all approved United States person

¹⁰ (U) NSA released these internal procedures in response to a Freedom of Information (FOIA) case filed in the U.S. District Court, Southern District of New York, ACLU v. National Security Agency, et al. (hereafter the ACLU FOIA), and they were posted, in redacted form, on ODNI's *IC on the Record* on April 11, 2017.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

identifiers to ensure compliance with NSA's minimization procedures.¹¹ For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the duration for which the United States person identifier has been authorized to be used as a query term, and any other relevant information. In addition, with respect to queries of Section 702-acquired *metadata* using a United States person identifier, NSA's internal procedures require that NSA analysts document the basis for each metadata query prior to conducting the query. NSD reviews the documentation for 100% of the metadata queries that NSA provides to NSD.¹²

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be incidents of non-compliance. For example, NSA is required to report *all* instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target's travel to the United States.¹³ The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. Investigations of all of these incidents sometimes result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) II. Joint Oversight of FBI

(U) FBI fulfills various roles in the implementation of Section 702, which are set forth in further detail in the Appendix. First, FBI is authorized under the certifications to acquire foreign intelligence information. Those acquisitions must be conducted pursuant to FBI's Section 702 targeting procedures.

¹¹ (U) On May 4, 2018, the DNI publicly released ODNI's fifth annual Transparency Report[s]: *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2017* (hereafter the *2017 Transparency Report*). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(A)), the *2017 Transparency Report* provided the "estimated number of search terms concerning a known United States person used to retrieve the unminimized contents of communications obtained under Section 702" (emphasis added) for the entire calendar year of 2017. On April 30, 2019, ODNI released the 6th annual transparency report for calendar year 2018.

¹² (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(B)), the *2017 Transparency Report* provided the "estimated number of queries concerning a known United States person used to retrieve the unminimized noncontents [(i.e. metadata)] information obtained under Section 702" (emphasis added) for the entire calendar year of 2017.

¹³ (U) If NSA had no prior knowledge of the target's travel to the United States and, upon learning of the target's travel, immediately "detasked" (i.e. stopped collection against) the target's facility, as is required by NSA's targeting procedures, the collection while the target was in the United States would not be considered a compliance incident under NSA's targeting procedures, although the collection would generally be subject to purge under the applicable minimization procedures. The joint oversight team carefully considers, and where appropriate, obtains additional facts regarding every reported detasking decision to ensure that NSA's tasking and detasking complied with its targeting and minimization procedures.

~~TOP SECRET//SI//NOFORN/FISA~~

~~(S//NF)~~ Second, FBI also [REDACTED]

[REDACTED] Pursuant to its own authority, FBI is authorized to [REDACTED] from electronic communication service providers by targeting facilities that NSA designates (hereinafter “Designated Accounts”). FBI conveys [REDACTED] from the electronic communications service providers [REDACTED] for processing in accordance with the agencies’ FISC-approved minimization procedures.

~~(S//NF)~~ Third, FBI may receive [REDACTED]¹⁴ unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI’s Section 702 minimization procedures. As described below, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

(U) NSD and ODNI’s oversight program is designed to ensure FBI’s compliance with statutory and procedural requirements for each of those three roles. NSD and ODNI generally conduct monthly reviews at FBI headquarters of FBI’s compliance with its targeting procedures and bimonthly reviews at FBI headquarters of FBI’s compliance with its minimization procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews at FBI Headquarters were conducted on the dates shown in Figure 2.

(U) Figure 2: FBI Reviews

UNCLASSIFIED

Date of FBI Onsite Review	Targeting and Minimization Reviewed
August 2 and 3, 2017	June 2017 targeting decisions
September 6 and 7, 2017	July 2017 targeting decisions
October 3 and 4, 2017	August 2017 targeting decisions; June 1, 2017 – August 31, 2017, minimization decisions
November 1 and 2, 2017	September 2017 targeting decisions
December 12 and 13, 2017	October 2017 targeting decisions; September 1, 2017 – -November 30, 2017, minimization decisions
January 17 and 18, 2018	November 2017 targeting decisions

(U) Figure 2 is UNCLASSIFIED.

(U) In conducting the targeting review, the joint oversight team reviews the targeting checklist completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.¹⁵ The joint oversight team also reviews a sample of other files to

¹⁴ [REDACTED]

¹⁵ ~~(S//NF)~~ If FBI’s application of its targeting procedures to [REDACTED] returns information from the databases discussed in FBI’s targeting procedures, then FBI provides a checklist that shows the results of its database queries. If FBI’s database queries returned results that FBI identifies as relevant to the target’s location or

~~TOP SECRET//SI//NOFORN/FISA~~

identify any other potential compliance issues. FBI analysts, supervisory personnel, and attorneys from FBI's National Security and Cyber Law Branch (NSCLB) are available to answer questions and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

(U) At the FBI reviews, with respect to minimization, the joint oversight team reviews documents related to FBI's application of its Section 702 minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations by the relevant FBI headquarters unit of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States person information.

(U) In addition to conducting minimization reviews at FBI headquarters, during this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention, query, and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During those field office reviews, NSD reviewed a sample of retention decisions made by FBI personnel in Section 702 cases and a sample of disseminations of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons. NSD also reviewed a sample of queries by FBI personnel in FBI systems that contain raw (unminimized) FISA-acquired information, including Section 702-acquired information. Those reviews ensure that the queries complied with the requirements in FBI's FISA minimization procedures, including its Section 702 minimization procedures.¹⁶ In addition, as a result of a Court-ordered reporting requirement in the FISC's *November 6, 2015 Memorandum Opinion and Order*¹⁷ for queries conducted after December 4, 2015, NSD reviews those queries to determine if any such queries were conducted solely for the purpose of returning evidence of a crime. If such a query was conducted, NSD would seek additional information as to whether FBI personnel received and reviewed Section 702-acquired information of or concerning a United States person in response to such a query. Pursuant to the FISC's opinion and order, such queries must subsequently be reported to the FISC.

(U) As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at 13 FBI field offices during this reporting period and reviewed

citizenship status, then FBI also provides the joint oversight team with supporting documentation [REDACTED]

[REDACTED] The joint oversight team currently reviews all checklists and supporting documentation provided by FBI for approved requests.

¹⁶ (U) The query requirements for FBI are currently contained in FBI's Section 702 amended Query Procedures (dated August 2019) for the 2018 Certifications, which are posted on *IC on the Record* on October 8, 2019. The Section 702 Query Procedures were not applicable to this joint assessment's reporting period.

¹⁷ (U) The FISC's November 6, 2015 Opinion and Order approved the 2015 FISA Section 702 Certifications. On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, this *Opinion and Order* on the ODNI public website *IC on the Record*.

~~(S//NF)~~ The title of the FISC's November 6, 2015 opinion is [REDACTED]

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

cases involving Section 702-tasked facilities.¹⁸ ODNI joined NSD at a subset of those reviews; ODNI received written summaries regarding all of the reviews from NSD regardless of whether ODNI was in attendance. Those reviews are further discussed in Section IV below.

~~(S//NF)~~ Separately, in order to evaluate the FBI's [REDACTED] acquisition [REDACTED] and provision of [REDACTED] the joint oversight team conducts an annual process review with FBI's technical personnel to ensure that those activities complied with applicable minimization procedures. The last annual process review occurred in May 2019.

~~(S//NF)~~ As further described in detail in Appendix A, FBI nominates potential Section 702 targets to NSA. [REDACTED]

[REDACTED] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in Appendix A.

(U) The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting and minimization procedures, the Attorney General's Acquisition Guidelines, or other agencies' procedures in which FBI is involved.¹⁹ Those investigations are coordinated with FBI OGC and may involve requests for further information; meetings with FBI legal, analytical, and/or technical personnel; or review of source documentation. Compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) III. Joint Oversight of CIA

(U) As further described in detail in the Appendix, although CIA does not directly engage in targeting or acquisition, it does nominate potential Section 702 targets to NSA. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team conducts onsite visits at CIA, and includes the results of those visits in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities.

(U) The onsite reviews also focus on CIA's application of its Section 702 minimization procedures. Reports for each of those reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews at CIA were conducted on the dates shown in Figure 3.

¹⁸ ~~(S//NF)~~ During those field office reviews, NSD reviewed [REDACTED] cases involving Section 702-tasked facilities.

¹⁹ (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) Figure 3: CIA Reviews****UNCLASSIFIED**

Date of CIA Onsite Review	Minimization Reviewed
September 27 and 29, 2017	June 1, 2017 – July 31, 2017
November 15 and 22, 2017	August 1, 2017 – September 30, 2017
January 17 and 19, 2018	October 1, 2017 – November 30, 2017

(U) Figure 3 is UNCLASSIFIED.

(U) As a part of the onsite reviews, the joint oversight team examines documents related to CIA's retention, dissemination, and querying of Section 702-acquired data. The team reviews a sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with CIA personnel issues involving the proper application of CIA's minimization procedures. The team also reviews all disseminations of information acquired under Section 702 that CIA identified as potentially containing United States person information. In addition, NSD and ODNI review CIA's written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications to assess whether those queries were compliant with CIA's minimization procedure requirements that such queries are reasonably likely to return foreign intelligence information, as defined by FISA.²⁰

~~(S//NF)~~ CIA may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. Additionally, and as further described in detail in the Appendix, CIA nominates potential Section 702 targets to NSA. [REDACTED]

[REDACTED] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [REDACTED], the results of those visits are included in the bimonthly NSA review reports discussed previously. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in the Appendix.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA's minimization procedures, the Attorney General

²⁰ (U) The query requirements for CIA are currently contained in CIA's Section 702 Query Procedures for the 2018 Certifications, which are posted on *IC on the Record* on October 8, 2019. The Section 702 Query Procedures were not applicable to this joint assessment's reporting period.

~~(S//NF)~~ As of [REDACTED], CIA had [REDACTED], such that NSD and ODNI will be able to review CIA's written foreign intelligence justifications for queries using United States person identifiers of the noncontents of unminimized Section 702-acquired communications. NSD and ODNI's assessments of such queries will be included in future joint assessments, as appropriate.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

Acquisition Guidelines, or other agencies' procedures in which CIA is involved.²¹ Investigations are coordinated through the CIA FISA Program Office and CIA's Office of General Counsel (CIA OGC), and when necessary, may involve requests for further information, meetings with CIA legal, analytical and/or technical personnel, or the review of source documentation. All compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) IV. Joint Oversight of NCTC

(U) As noted above, NCTC previously played a more limited role in implementing Section 702, as reflected in the "Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended." During this reporting period, NCTC was authorized to receive unminimized Section 702 data and also had access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism. As part of the joint oversight of NCTC to ensure compliance with these procedures, NSD and ODNI conduct reviews of NCTC's access, receipt, and processing of minimized Section 702 information received from FBI. NSD conducted a review of minimized Section 702 information received from FBI for this reporting period in May 2017.

~~(S//NF)~~ As referenced in footnote 4, during the prior reporting period, NCTC was authorized to receive unminimized Section 702 information pertaining to counterterrorism. NCTC's processing, retention, and dissemination of such information is subject to its 2016 Minimization Procedures, which the FISC approved in April 2017. Unlike NSA, FBI, and CIA, NCTC does not directly engage in targeting or acquisition, nor does it nominate potential Section 702 targets to NSA. NCTC may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to NCTC's minimization procedures. NCTC has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Because NCTC now acquires unminimized Section 702 information, the joint oversight team conducts onsite visits at NCTC, and the results of those visits are included in bimonthly NCTC review reports.

(U) The onsite reviews focus on NCTC's application of its Section 702 minimization procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews at NCTC were conducted on the dates shown in Figure 4.

²¹ (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve CIA.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) Figure 4: NCTC Reviews****UNCLASSIFIED**

Date of NCTC Onsite Review	Minimization Reviewed
July 21, 2017	May 24, 2017 ²² – June 30, 2017
September 18, 2017	July 1, 2017 – August 31, 2017
November 17, 2017	September 1, 2017 – October 31, 2017
January 19, 2018	November 1, 2017 – December 31, 2017

(U) Figure 4 is UNCLASSIFIED.

(U) As a part of the onsite review, the joint oversight team examines documents related to NCTC's retention, dissemination, and querying of Section 702-acquired data. The team reviews all communications acquired under Section 702 that have been minimized and retained by NCTC, irrespective of whether it contains United States person information. Reviewers ensure that communications have been properly minimized and discuss with personnel issues involving the proper application of NCTC's minimization procedures. The team also reviews all NCTC disseminations of information acquired under Section 702. In addition, NSD and ODNI review NCTC's written foreign intelligence justifications for all queries of the content of unminimized Section 702-acquired communications.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with NCTC's minimization procedures or other agencies' procedures in which NCTC is involved.²³ Investigations are coordinated through the NCTC Compliance and Transparency Group and NCTC Legal, a forward deployment component of the ODNI Office of General Counsel (ODNI OGC), and when necessary, may involve requests for further information; meetings with NCTC Legal, analytical, and/or technical personnel; or the review of source documentation. All compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) V. Interagency/Programmatic Oversight

(U) Because the implementation and oversight of the Government's Section 702 authorities are a multi-agency effort, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence, and comply with all legal requirements. For those reasons, NSD and ODNI generally conduct twice monthly telephone calls and quarterly meetings (in addition to ad hoc calls and meetings on specific topics as needed) with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures. Additionally, NSD and ODNI conduct

²² ~~(S//NF)~~ NCTC began receiving unminimized Section 702-acquired information [REDACTED]

²³ (U) Insofar as NCTC reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve NCTC.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

weekly telephone calls with NSA to address outstanding compliance matters and work through the process of understanding those matters and reporting incidents to the FISC.

(U) NSD and ODNI's programmatic oversight also involves efforts to proactively minimize the number of incidents of noncompliance. For example, NSD and ODNI have required agencies to demonstrate to the joint oversight team new or substantially revised systems involved in Section 702 targeting or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review and, where appropriate, seek modifications of their targeting and minimization procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance.

(U) VI. Training

(U) In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have also continued their training efforts to ensure compliance with the targeting and minimization procedures. NSA continued to administer the compliance training course updated in November 2016.²⁴ All NSA personnel who require access to Section 702 data are required to complete this course on an annual basis in order to gain and/or maintain that access. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders and compliance advisories to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. Those training reminders and compliance advisories are e-mailed to individual analysts and targeting adjudicators and maintained on internal agency websites²⁵ where personnel can obtain information about specific types of Section 702-related issues and compliance matters.

(U) FBI has similarly continued implementing its online training programs regarding Section 702 nominations, minimization, and other related requirements. Completion of those FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI have also conducted in-person trainings at multiple FBI field offices. For example, during this reporting period, NSD and FBI continued to provide additional focused training at FBI field offices on the Section 702 minimization procedures, including training FBI field personnel on the attorney-client privileged communication provisions and query requirements of FBI's minimization procedures.²⁶ NSD training at FBI field offices also included training on the reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications. As discussed above, this reporting

²⁴ (U) The transcript associated with this training, dated August 2016, was posted, in redacted form, on *IC on the Record* on August 22, 2017, in response to the aforementioned ACLU FOIA case titled, *OVSC1203: FISA Amendments Act Section 702* (Document 17, NSA's Training on FISA Amendments Act Section 702).

²⁵ (U) These documents were posted, in redacted form, on ODNI's *IC on the Record* on August 23, 2017, in response to the aforementioned ACLU FOIA case: *NSA's 702 Targeting Review Guidance* (Document 10), *NSA's 702 Practical Applications Training* (Document 11), *NSA's 702 Training for NSA Adjudicators* (Document 12), and *NSA's 702 Adjudication Checklist* (Document 13).

²⁶ (U) This specific training began before, occurred during, and continued after the current reporting period of June 1, 2017 – November 30, 2017.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN//FISA~~

requirement applies to queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a United States person that was reviewed by FBI personnel. Additionally, while outside this assessment's reporting period, the FBI is developing new training modules pertaining to querying; an update to this training will be provided in the applicable joint assessment.

(U) CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a required training program for anyone handling raw Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Furthermore, CIA has issued guidance to its personnel about how to properly conduct United States person queries that are reasonably likely to return foreign intelligence information, *see USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data*.²⁷

(U) NCTC provides training on the NCTC Section 702 Minimization Procedures to all of its personnel who may have access to raw Section 702-acquired information. NCTC uses a training tracking system through which NCTC can verify that its users have received the appropriate Section 702 training before being given access to raw Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed raw Section 702-acquired information in its system to confirm that those personnel who access raw Section 702-acquired information had received training on the NCTC Section 702 Minimization Procedures.

(U) SECTION 3: TRENDS IN SECTION 702 TARGETING AND MINIMIZATION

(U) In conducting the above-described oversight program, NSD, ODNI, and the agencies have collected a substantial amount of data regarding the implementation of Section 702. In this section, a comprehensive collection of this data has been compiled in order to identify overall trends in the agencies' targeting, minimization, and compliance.

(U) I. Trends in NSA Targeting and Minimization

(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,²⁸ the figure charting the average number of facilities under

²⁷ (U) As discussed in the previous Joint Assessment, in response to the aforementioned ACLU FOIA case, CIA's guidance document was posted, in redacted form, on ODNI's *IC on the Record* on April 11, 2017, *see* ACLU April 2017 Production 5, Document 15 "CIA's United States Person Query Guidelines for Personnel."

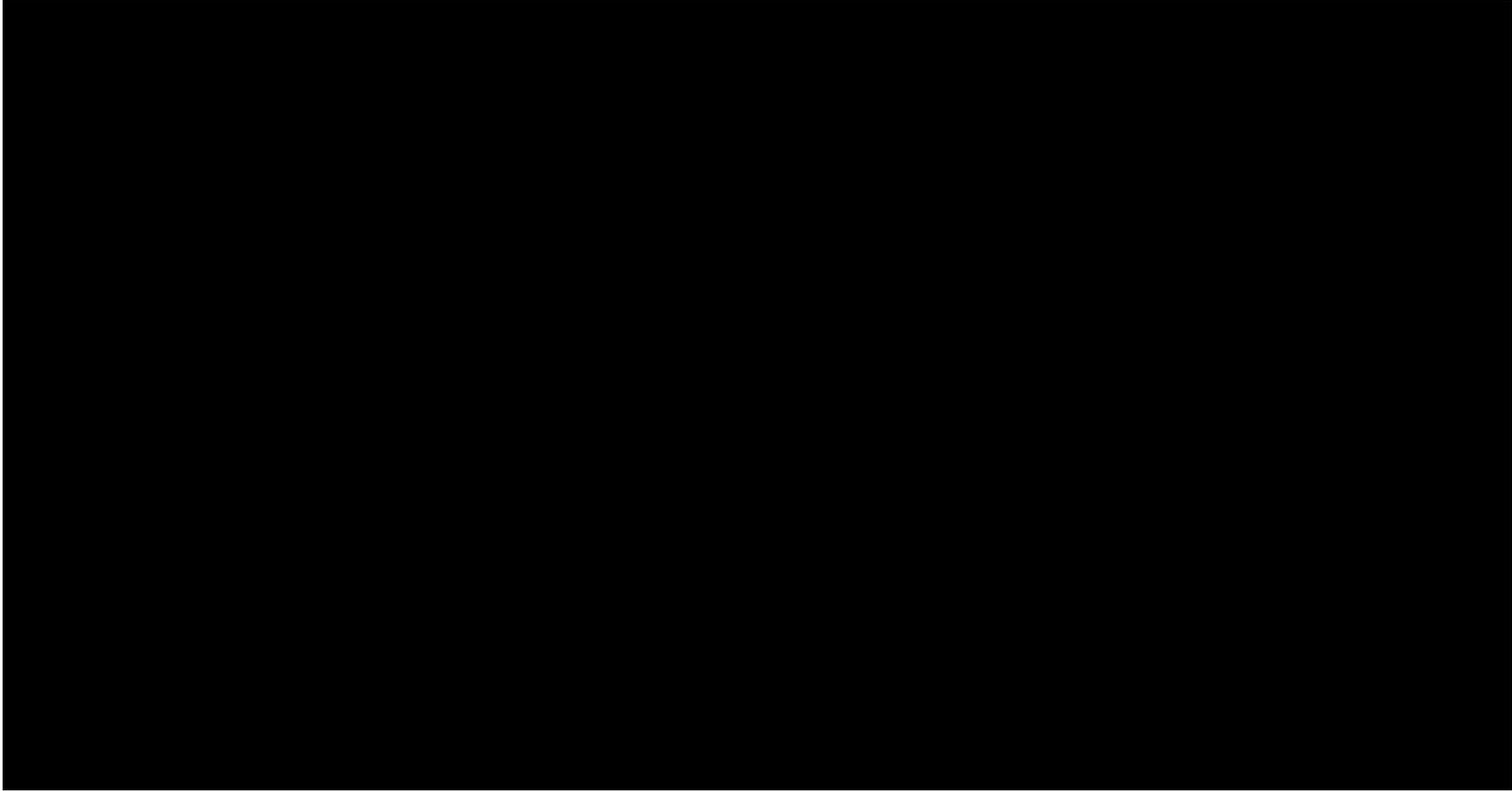
²⁸ (U) The provided number of facilities, on average, subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released by the ODNI most recently in its *2017 Transparency Report*. The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified numbers provided in the Transparency Report estimate the number of Section 702 *targets*. As noted in the Transparency Report, the number of 702 "targets" reflects an estimate of the number of known users of particular facilities, subject to intelligence collection under those Certifications. The

~~TOP SECRET//SI//NOFORN//FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.²⁹

(U) Figure 5: Average Number of Facilities Under Collection



(U) Figure 5 is classified TOP SECRET//SI//NOFORN

~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [REDACTED] facilities were under collection pursuant to the applicable certifications on any given day during the reporting period.³⁰ This represents a 23.1% increase from the approximately [REDACTED] facilities under collection on any given day in the last reporting period. [REDACTED]

classified number of facilities account for those facilities subject to Section 702 acquisition *during the current six month reporting period*, whereas the Transparency Report estimates the number of targets affected by Section 702 *during the calendar year*.

²⁹ (U) One of the reporting periods in which the total number of facilities under collection decreased occurred prior to 2010 and is not reflected in the Figure 4.

³⁰ ~~(S//NF)~~ The applicable certifications for this reporting period were [REDACTED]

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) The above statistics describe the *average* number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.³¹ Classified Figure 6 charts the total monthly numbers of newly tasked facilities since 2012.

(U) Figure 6: New Taskings by Month (Yearly Average for 2012 through 2016)



(U) Figure 6 is classified ~~TOP SECRET//SI//NOFORN~~.

~~(S//SI//NF)~~ Specifically, NSA provided documentation of approximately [REDACTED] new taskings during the reporting period. This represents a 19.8% increase in new taskings from the previous reporting period. [REDACTED]

³¹ (U) The term newly tasked facilities refers to any facility that was added to collection under a certification. This term includes any facility added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked facilities are facilities that had been previously tasked for collection, were detasked, and then retasked.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

~~(S//SI//NF)~~ From December 2016 through May 2017, NSA tasked an average of approximately [REDACTED] telephony facilities. From June 2017 through November 2017, NSA has tasked an average of approximately [REDACTED] telephony facilities. This represents a [REDACTED] increase in the average monthly telephony facilities when compared to the previous six months.

~~(S//SI//NF)~~ From December 2016 through May 2017, NSA tasked an average of approximately [REDACTED] electronic communications accounts. From June 2017 through November 2017, NSA tasked an average of approximately [REDACTED] electronic communication accounts (a [REDACTED] increase from the prior six month period).

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data and provided NSD and ODNI access to all reports NSA identified as containing United States person information.³² Figure 7 contains the classified number of serialized reports and reports identified as containing United States person information over the last ten reporting periods. The NSD and ODNI reviews revealed that the United States person information was at least initially masked in the vast majority of circumstances.³³ The number of serialized reports NSA has identified as containing United States person information decreased, after increasing for the prior reporting period.

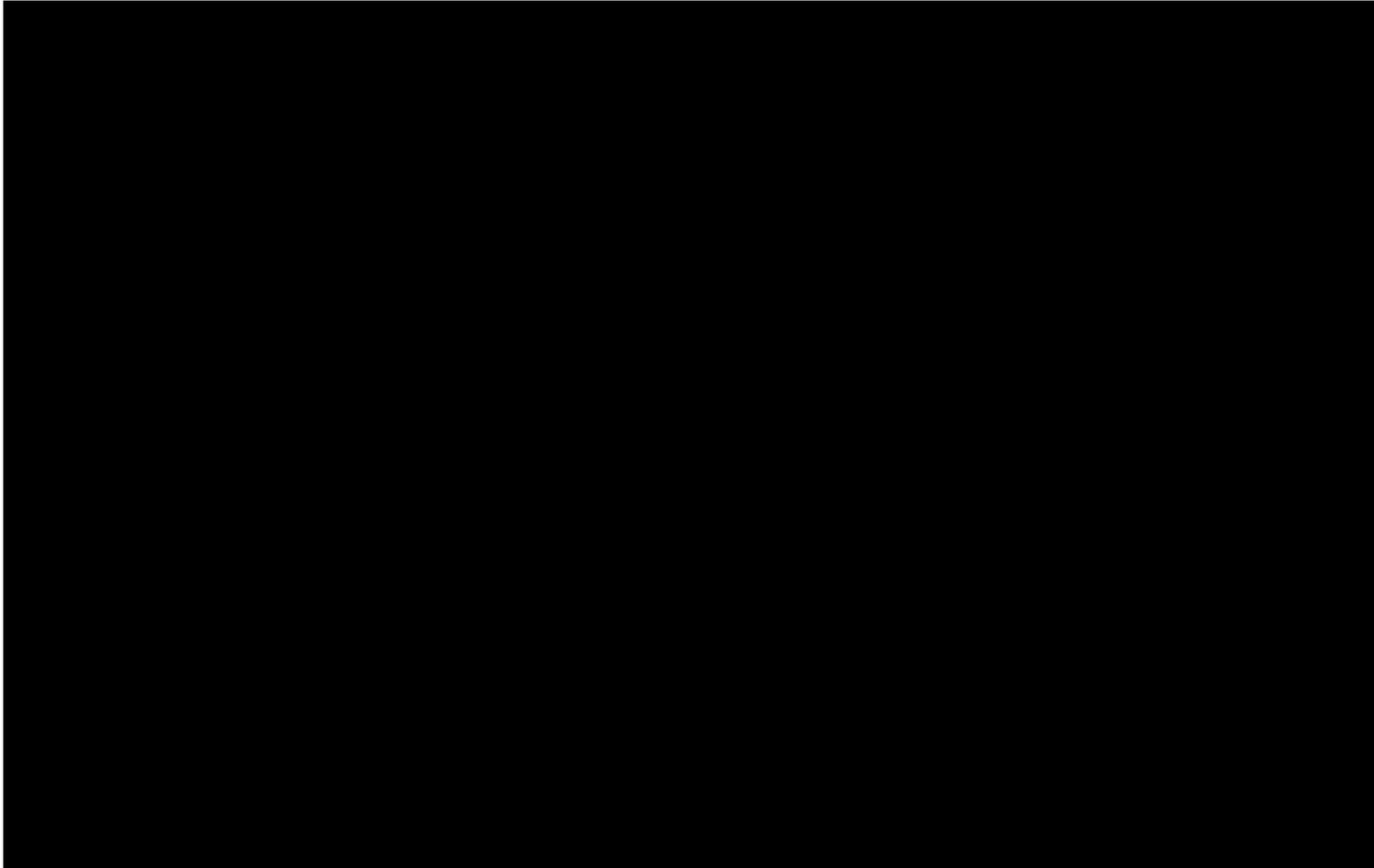
³² (U) Previous joint assessments referred to those reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. However, given that Section 702 of FISA replaced the PAA in 2008, the Government no longer disseminates minimized information that was previously acquired pursuant to PAA. However, Figure 6 provides a trend analysis over a longer period of time and may include reports containing minimized PAA-acquired information in addition to minimized Section 702-acquired information.

³³ (U) NSA generally “masks” United States person information by replacing the name or other identifying information of the United States person with a generic term, such as “United States person #1.” Agencies may request that NSA “unmask” the United States person identity. Prior to such unmasking, NSA must determine that the United States person’s identity meets the applicable standards in NSA’s minimization procedures.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) Figure 7: Total Disseminated NSA Serialized Reports Based Upon Section 702- Acquired Data and Number of Such Reports NSA Identified as Containing USP Information



(U) Figure 7 is classified ~~TOP SECRET//SI//NOFORN/FISA~~.

~~(S//NF)~~ Specifically, in this reporting period NSA identified to NSD and ODNI approximately [REDACTED] serialized reports based upon minimized Section 702-acquired data. This represents a 0.8% increase from the approximately [REDACTED] serialized reports NSA identified in the prior reporting period. Figure 7 reflects NSA reporting over the last eleven reporting periods; the number of reports identified by NSA decreased in only one reporting period.

~~(S//NF)~~ Figure 7 also shows the number of these serialized reports that NSA identified as containing United States person information. During this reporting period, NSA identified approximately [REDACTED] serialized reports as containing United States person information derived from Section 702-acquired data.³⁴ The percentage of reports containing United States person information

³⁴ (U) NSA does not maintain records that allow it to readily determine, in the case of a report that includes information from several sources, from which source a reference to a United States person was derived. Accordingly, the references to United States person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

was lower this reporting period (7.3 %) than the 8.5% reported in the previous reporting period and lower than the 8.4% and 8.5% reported in the two prior reporting periods.

(U) II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA designated-facilities that FBI approved.³⁵ As detailed below, the number of facilities designated for acquisition has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.³⁶

(U) As classified Figure 8 details, FBI approves the vast majority of NSA's designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA-designated facilities have already been evaluated and found to meet the NSA targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion³⁷ were rejected on the basis that they were ineligible for Section 702 collection.

(U) In 2012 and 2013, the yearly average of designated facilities approved by FBI steadily increased. The yearly average of designated facilities approved by FBI in 2014 slightly decreased, and then increased again in 2015 and 2016. In the first eleven months of 2017, the number of designated facilities approved by FBI each month has varied. NSD and ODNI have continued to track the number of facilities approved by FBI in 2017 and will incorporate this information into future Joint Assessments.

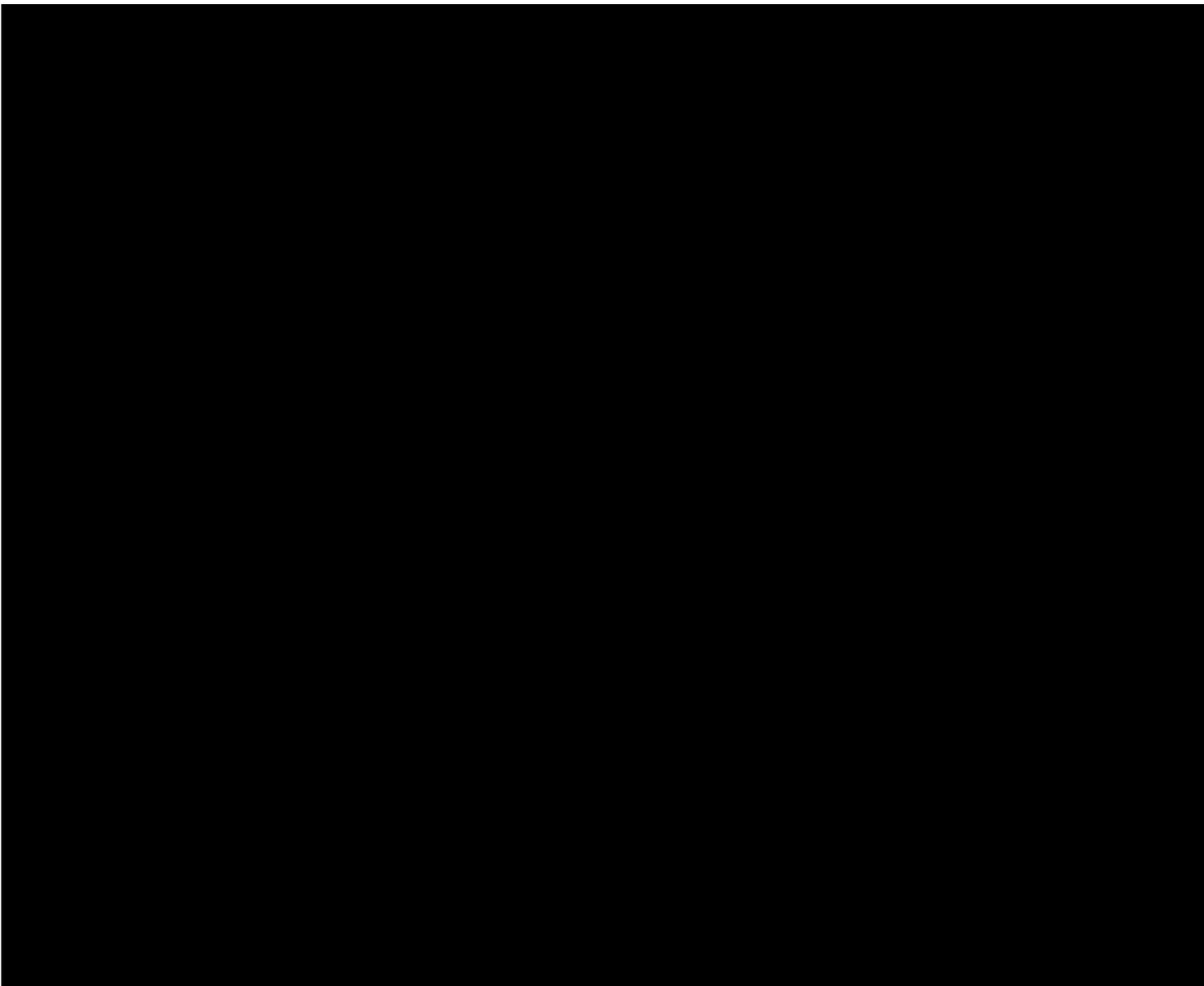
35

36

37

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~



(U) Figure 8 is classified [REDACTED]

~~(S//SI//NF)~~ Specifically, FBI reports that NSA designated approximately [REDACTED] accounts [REDACTED] during the reporting period – an average of [REDACTED] designated accounts per month. This is a [REDACTED] decrease from the approximately [REDACTED] accounts designated in the prior six-month reporting period. [REDACTED]



~~(S//NF)~~ FBI approved [REDACTED] requests [REDACTED]



~~TOP SECRET//SI//NOFORN/FISA~~

(U) As indicated in prior Joint Assessments, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its dissemination of Section 702-acquired information from FBI headquarters to FBI field offices. NSD conducts oversight reviews at multiple FBI field offices each year, some of which ODNI attends, and during those reviews, NSD reviews a sample of the Section 702 disseminations issued by the respective field office. Because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of Section 702-acquired United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. § 1881a(1)(3)(A)(i).

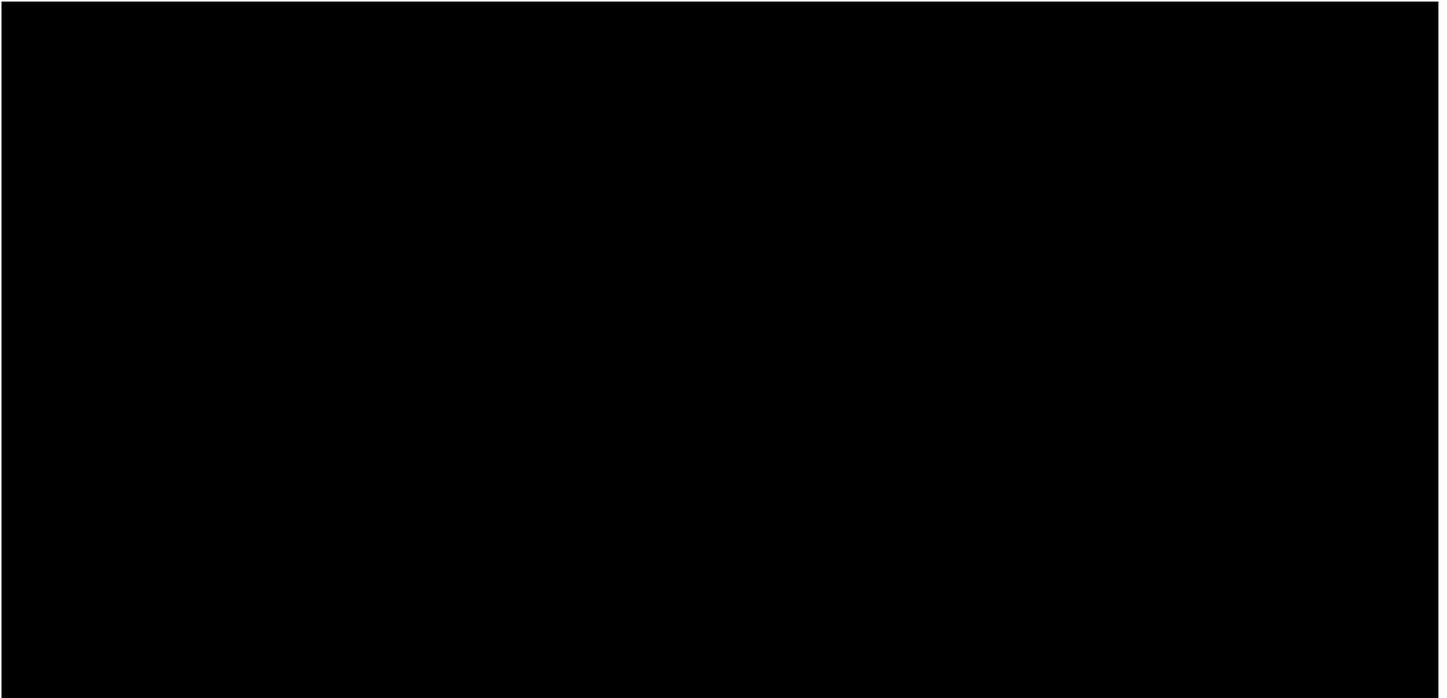
(U) III. Trends in CIA Minimization

(U) CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Classified Figure 9 compiles the number of such disseminations of reports containing United States person information identified in the last ten reporting periods (December 2012 – May 2013 through the current period of June 2017 – November 2017). In the first three reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the fourth reporting period, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the fifth and sixth reporting periods, the number of CIA-identified disseminations containing United States person information again decreased. In seventh through tenth reporting periods, the number of CIA-identified disseminations containing United States person information has varied, but remains objectively low.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) Figure 9: Disseminations Identified by CIA as Containing Minimized Section 702-Acquired United States Person Information (Excluding Certain Disseminations to NCTC)



(U) Figure 9 is classified ~~TOP SECRET//SI//NOFORN/FISA~~.

~~(S//NF)~~ During this reporting period, CIA identified approximately [REDACTED] disseminations of Section 702-acquired data containing minimized United States person information. This is a [REDACTED] increase from the approximately [REDACTED] such disseminations CIA made in the prior reporting period. [REDACTED], and as reported in prior Joint Assessments, CIA also permits some personnel [REDACTED]

[REDACTED] NSD and ODNI, however, review all [REDACTED] containing Section 702-acquired information that CIA has identified as potentially containing United States person information to ensure compliance with CIA's minimization procedures.

(U) CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. The CIA minimization procedures must be applied to those files before they are retained or transferred to systems with broader access.³⁸ Classified Figure 10 details the total number of files that were either retained or transferred, as well as the number of those retained or transferred files that contain identified United States person information. Beginning in the middle of the reporting period covered by the 13th Joint Assessment (dated September 2015), CIA began reporting the number of files CIA transferred to systems with broader access, instead of

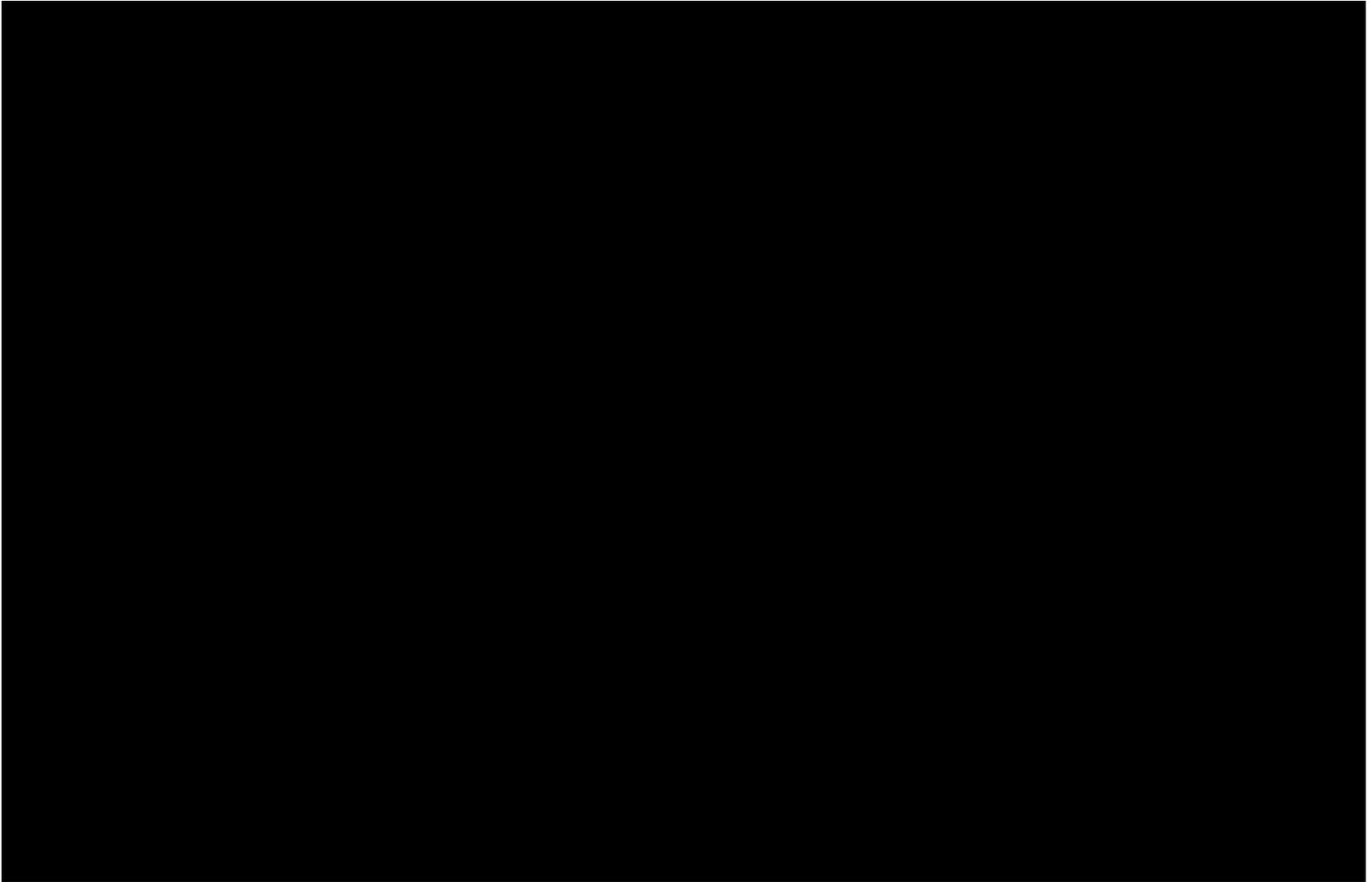
³⁸ ~~(S//NF)~~ [REDACTED]. In making those retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

the number of files retained in systems of limited access, as the number of transferred files provides a more accurate portrayal of CIA's use of Section 702-acquired information. This current assessment reports the total number of files CIA transferred from June 2017 through November 2017. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.³⁹ In all reporting periods, the number of retained or transferred files identified by CIA as potentially containing United States person information has been consistently a very small percentage of the total number of retained or transferred files.

(U) Figure 10: Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred Which Contained Potential United States Person Information



(U) Figure 10 is classified ~~SECRET//NOFORN~~.

~~TS//SI~~ For this reporting period, CIA analysts transferred a total of approximately [REDACTED] of which were identified by CIA as containing a communication n information. This is a [REDACTED] decrease in the number of files transferred or retained when compared with the previous reporting period when [REDACTED]

³⁹ [REDACTED]

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS**

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes. The compliance incidents during the reporting period represent a very small percentage of the overall collection activity.

(U) As noted in prior reports, in the cooperative environment the implementing agencies have established, an action by one agency can result in an incident of noncompliance with another agency's procedures. It is also important to note that a single incident can have broader implications. For example, a "NSA compliance incident" could be caused from typographical errors contained in another agency's nomination.

(U) Each of the compliance incidents for this current reporting period is described in detail in the corresponding Section 707 Report. This joint assessment does not reiterate the compliance incidents set forth in the Section 707 Report. It does, however, examine those incidents to assess broader implications and to determine whether the agency's corrective measures address those implications.

(U) Specifically, because even a small number of incidents can have the potential of carrying broader implications, the Joint Assessment provides NSD and ODNI's analysis of those compliance incidents in an effort to identify existing patterns or trends that might identify the underlying causes of those incidents. The joint oversight team then considers whether and how those underlying causes could be addressed through additional remedial or proactive measures and assesses whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures, some of which are detailed below, especially as it pertains to investigating whether additional and/or new system automation may assist in preventing compliance incidents.

(U) I. Compliance Incidents – General**(U) A. Statistical Data Relating To All Compliance Incidents**

~~(S//NF)~~ As noted in the Section 707 Report, there were a total of [REDACTED] compliance incidents that involved noncompliance with NSA's targeting or minimization procedures and [REDACTED] compliance incidents involving noncompliance with FBI's targeting and minimization procedures, for a total of [REDACTED] incidents involving NSA and/or FBI procedures.⁴¹ During this reporting period, there were [REDACTED] identified incidents of noncompliance with CIA's minimization procedures. There was one

⁴¹ (U) As is discussed in the Section 707 report and herein, some compliance incidents involve more than one element of the IC. Incidents have therefore been grouped not by the agency "at fault," but instead by the set of procedures with which actions have been noncompliant.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

incident of noncompliance with NCTC’s minimization procedures. In addition, there were [REDACTED] identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

(U) Figure 12 puts those compliance incidents – for all four agencies – in the context of the average number of facilities subject to acquisition on any given day⁴² during the reporting period:

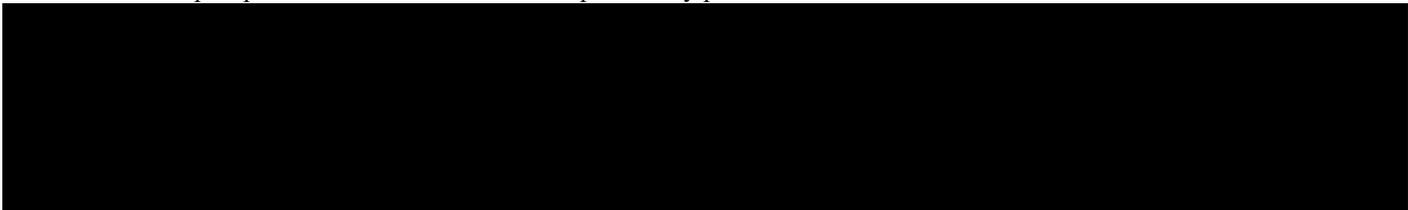
(U) Figure 12: Overall Compliance Incident Rate

TOP SECRET//SI//NOFORN	
(U) All compliance incidents during reporting period (June 1, 2017 – November 30, 2017)	[REDACTED]
(U) Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
(U) Overall compliance incident rate: number of incidents divided by average facilities subject to acquisition	(U) 0.42%

(U) Figure 12 is classified ~~TOP SECRET//SI//NOFORN~~

(U) The overall compliance incident rate continues to remain below one percent, with the current rate of 0.42% representing an increase from the 0.37% overall compliance incident rate in the prior reporting period. However, the number of notification delays more than doubled during this reporting period, when compared to the prior reporting period. As discussed below, notification delays are incidents in which the violation is that the notification requirement contained in the targeting procedures was not satisfied. Substantive compliance incidents are not captured in this metric. If a compliance incident involved both a substantive error (for example, a tasking or detasking error) and the failure to meet the notification requirement, the substantive error was counted separate from the notification delay. For the majority of these incidents, the only incident of non-compliance was the failure to comply with the notification requirement. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is 0.34%. This information is explained below and detailed in Figure 13.

⁴² (S//NF) [REDACTED] The Attorney General’s Section 707 report provides further details with respect to any particular incident.

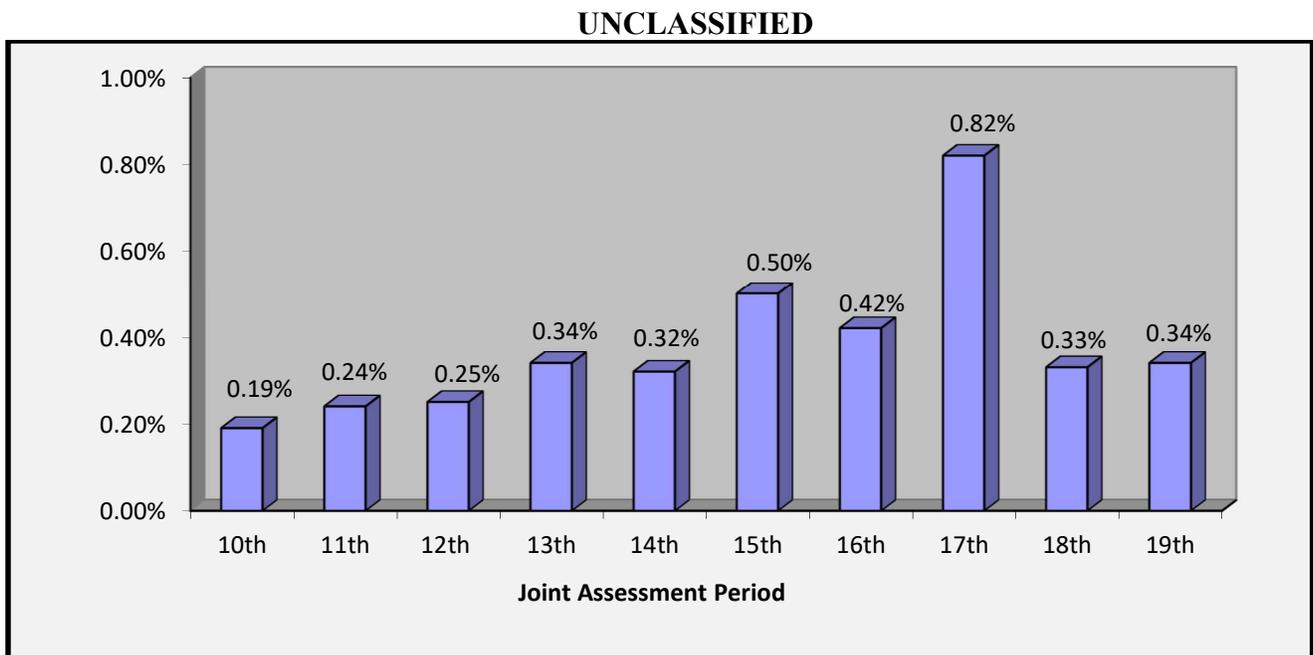


~~TOP SECRET//SI//NOFORN/FISA~~

(U) While the incident rate remains well below one percent, this percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States person information.

(U) As part of the oversight team’s periodic evaluation of the tools to assess compliance, the joint oversight team, as explained in past Joint Assessments, determined that another measure is to compare the overall compliance incident rate excluding notification delays. Figure 13 shows that adjusted rate:

(U) Figure 13: Overall Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), *not* including Notification Delays



(U) Figure 13 is UNCLASSIFIED.

(U) As Figure 13 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.34%, which is almost the same as what was reported in the prior reporting period (0.33%), and still below 1%. While the underlying causes of the compliance incident rate are discussed later in this assessment, as the DNI explained on June 7, 2017, during an open hearing in front of the Senate Select Committee on Intelligence, ODNI and DOJ's reviews have revealed an extremely low incident rate. The DNI explained that, while mistakes have occurred, “any system with zero compliance incidents is a broken compliance system because humans make mistakes.” The DNI emphasized that when the government finds compliance incidents, those incidents are reported and corrected.

(U) The joint oversight team assesses that the consistently low compliance incident rate is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures.

~~TOP SECRET//SI//NOFORN/FISA~~

(U) As explained in previous assessments, in seeking to assess the value of such statistical data, the oversight team periodically evaluates how and what data it collects to provide for more meaningful statistics. For example, the team considers whether there are other means of comparison – whether with the currently tracked actions or by implementing the tracking of certain other data – that could provide a more comprehensive understanding of overall compliance. The Joint Assessment has traditionally compared the number of compliance incidents (*i.e.*, the “numerator”) to targeting activity during the reporting period, which is reflected as the number of average tasked facilities (*i.e.*, the “denominator”). Using the number of average facilities subject to acquisition during the reporting period as the denominator provides a general proxy for an activity level that is relevant from a compliance perspective. That is, the joint oversight team believes that the number of targeted facilities generally comports with the number of activities that could result in compliance incidents (*e.g.*, taskings, detaskings, disseminations, and queries).

(U) While tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint, it remains a proxy. A potential flaw with using this particular proxy is that the analysis of the type of incidents in the numerator does not always match to the targeting activity in the denominator. For example, assessing a delayed *detasking* incident (which is an incident resulting from non-compliance with targeting procedures) as contained in the numerator to the number of average *tasked* facilities as contained in the denominator compares closely similar factors – both are directly related to tasking and must meet the requirements of the targeting procedures. However, the factors become less similar when assessing an improper *querying* incident or an improper *dissemination* (which are incidents resulting from non-compliance with minimization procedures) to the number of average *tasked* facilities – here the incident implicates the requirements of the minimization procedures whereas the tasking of the facility implicates the requirements of the targeting procedures. Conceivably, those minimization incidents should be compared to the number of total minimization actions, but we are unable to count or track minimization actions in that manner. Adding to the dissimilarity is that multiple agencies’ (NSA, FBI, CIA, and NCTC) incidents – as well as incidents by service providers – are counted in the overall compliance incident rate, but only two agencies (NSA and FBI) actually conduct targeting activity pursuant to their respective targeting procedures.

(U) However, while assessing that the agencies remain overall compliant, the oversight team revisited the value of the overall incident rate proxy and determined that providing a new comparison rate would enhance overseers’ (the FISC, Congress, and the PCLOB) and the public’s understanding of Section 702 compliance. While the new comparison is offered below, for consistency in evaluating long-term trends, the joint assessments will continue to provide the overall compliance incident rates in figures 12 and 13 above. However, understanding the limits of that proxy, this assessment now begins providing a new metric: NSA targeting compliance incident rate going forward in time from this Joint Assessment’s reporting period because, as explained below, most incidents involved NSA’s procedures (see Figures 15 and 16).

(U) Separating the targeting errors from the minimization errors allows for another layer of evaluation. We provide these new metrics to advance the understanding of the incidents’ impact and the causes of those incidents. The new metrics are provided after an explanation of the categories of compliance incident so that the new metrics can better be understood.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) B. NSA's Compliance Incidents: Categories and Number of Incidents**

(U) As it has been historically, most of the compliance incidents occurring during this reporting period involved non-compliance with the NSA's targeting or minimization procedures. This largely reflects the centrality of NSA's targeting and minimization efforts in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting or minimization procedures have generally fallen into the categories below. However, in some instances, an incident may involve more than one category of noncompliance.

(U) Incidents of non-compliance with NSA's Targeting Procedures:

- (U) *Tasking Issues*. This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.
- (U) *Detasking Issues*. This category involves incidents in which the facility was properly tasked in accordance with the targeting procedures, but errors in the detasking of the facility caused noncompliance with the targeting procedures.
- (U) *Overcollection*. This category involves incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection."
- (U) *Notification Delays*. This category involves incidents in which a notification requirement contained in the targeting procedures was not satisfied.⁴³
- (U) *Documentation Issues*. This category involves incidents where the determination to target a facility was not properly documented as required by the targeting procedures.

(U) Incidents of non-compliance with NSA's Minimization Procedures:

- (U) *Minimization Issues*. This category involves NSA's compliance with its minimization procedures.

(U) *Other Issues*. This category involves incidents that do not fall into one of the six above categories. In these instances, the joint oversight team will assess each incident to determine if it resulted from non-compliance with NSA's targeting procedures or with NSA's minimization procedures and account for those incidents accordingly.

(U) While the above categories specifically pertain to NSA incidents, the FBI's targeting incidents categories and all agencies' minimization incidents categories generally align to those

⁴³ (U) As explained above, a compliance incident may involve both a failure to meet the notification requirement and a substantive error (for example, a tasking or detasking error). However, in those instances, the substantive error was counted separate from the notification delay. For the majority of delayed notification incidents, the only incident of non-compliance was the failure to comply with the notification requirement.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

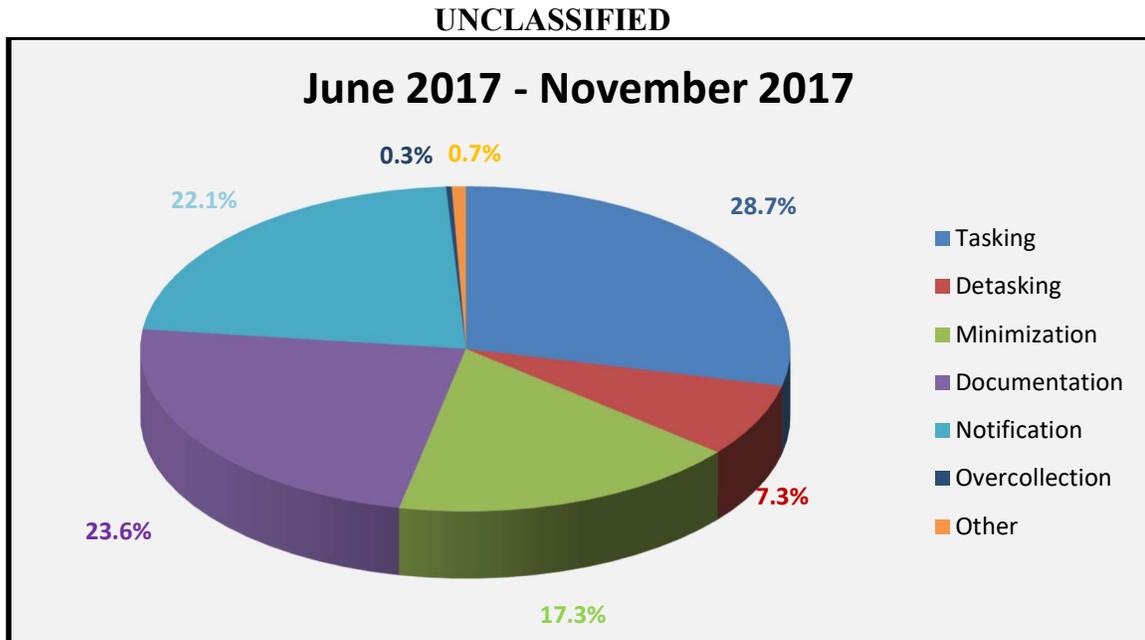
NSA categories. Because only NSA and FBI are permitted to target pursuant to Section 702, only NSA and FBI have targeting procedures (which have been publicly released). All four agencies have minimization procedures (which have been publicly released). Compliance incidents by FBI, CIA, and NCTC are discussed in their respective sections below.

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 14A depicts the percentage of NSA compliance incidents in each category that occurred during this reporting period, whereas Figure 14B provides that actual classified number of NSA incidents.

~~TOP SECRET//SI//NOFORN/FISA~~

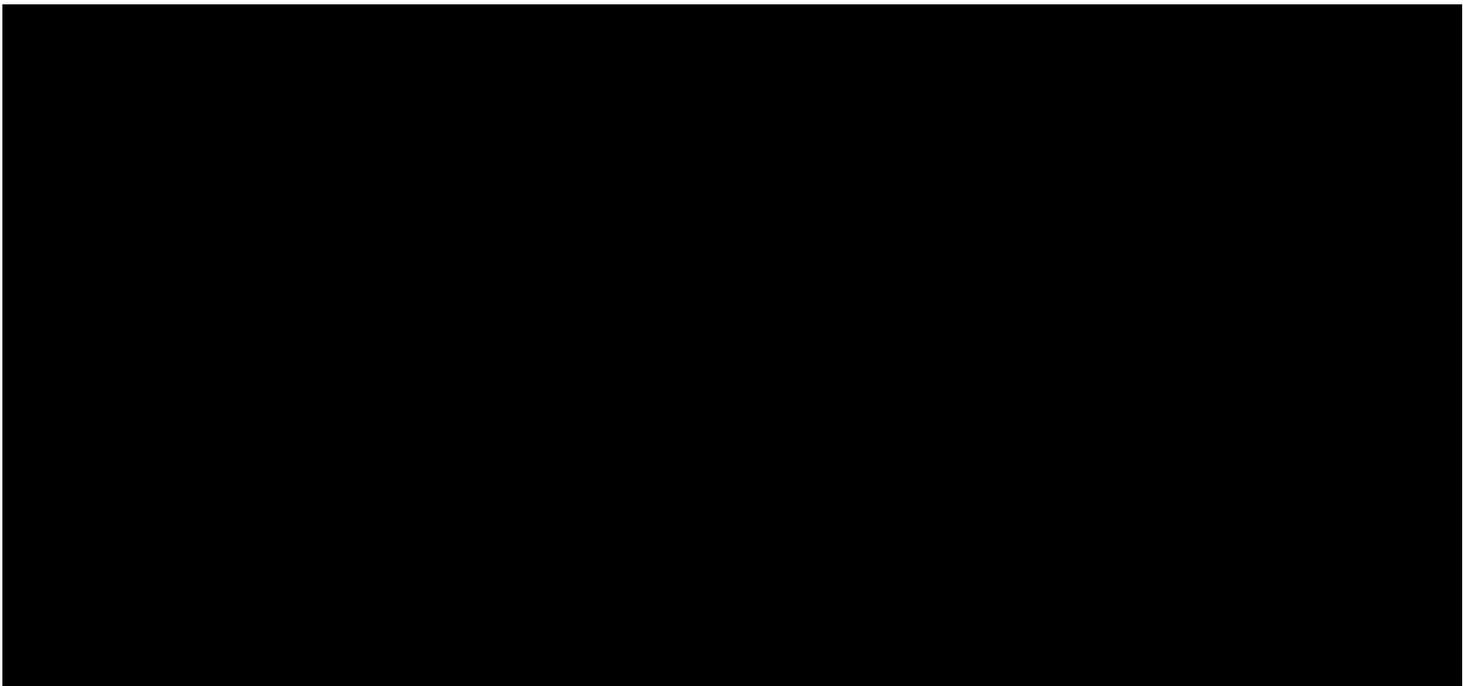
~~TOP SECRET//SI//NOFORN/FISA~~

(U) Figure 14A: Percentage Breakdown of Compliance Incidents Involving the NSA Targeting and Minimization Procedures



(U) Figure 14A is UNCLASSIFIED

(U) Figure 14B: Number of Compliance Incidents Involving the NSA Targeting and Minimization Procedures



(U) Figure 14B is classified ~~SECRET//NOFORN~~

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) As Figures 14A and 14B demonstrate, the largest proportion of incidents implicate non-compliance with the documentation and notification requirements of the targeting procedures. Tasking errors and detasking delays account for the next largest percentage of incidents, followed by minimization errors. Tracking the proportion of incidents allows for the joint assessment team to identify trends and to address the non-compliance with appropriate remedies. Being able to do so is important for a variety reasons, especially as it pertains to more substantive tasking and detasking compliance incidents that can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, the joint oversight team also focuses on incidents of noncompliance with minimization procedures because these types of incidents may involve information concerning United States persons.

~~(S//NF)~~ More specifically, for NSA, the number of tasking incidents increased from [REDACTED]; detasking incidents increased [REDACTED]; minimization incidents decreased from [REDACTED]; documentation incidents increased from [REDACTED]; and “other” category incidents decreased from [REDACTED]. The number of notification delays increased from [REDACTED]. There were [REDACTED] overcollection incidents in this period.

(U) Focusing on NSA’s targeting procedures, Figure 15 provides NSA targeting compliance incident rate beginning in this current reporting period. This new metric compares similar factors: NSA’s number of *targeting incidents* (i.e., the “numerator”) to the NSA’s targeting activity of the number of average *tasked facilities* (i.e., the “denominator”). The number of NSA’s targeting errors includes the following categories of incidents: tasking errors, detasking delays, documentation errors, notification delays, overcollection, and other. As explained above, incidents that fall under the “other issues” category may be included as well if those constituted errors in following NSA’s targeting procedures.

(U) Figure 15: NSA Targeting Compliance Incident Rate

TOP SECRET//SI//NOFORN	
(U) NSA compliance incidents relating to NSA’s targeting procedures, during reporting period (June 1, 2017 – November 30, 2017)	[REDACTED]
(U) Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
(U) NSA targeting compliance incident rate: number of targeting incidents divided by average facilities tasked to acquisition	(U) 0.28%

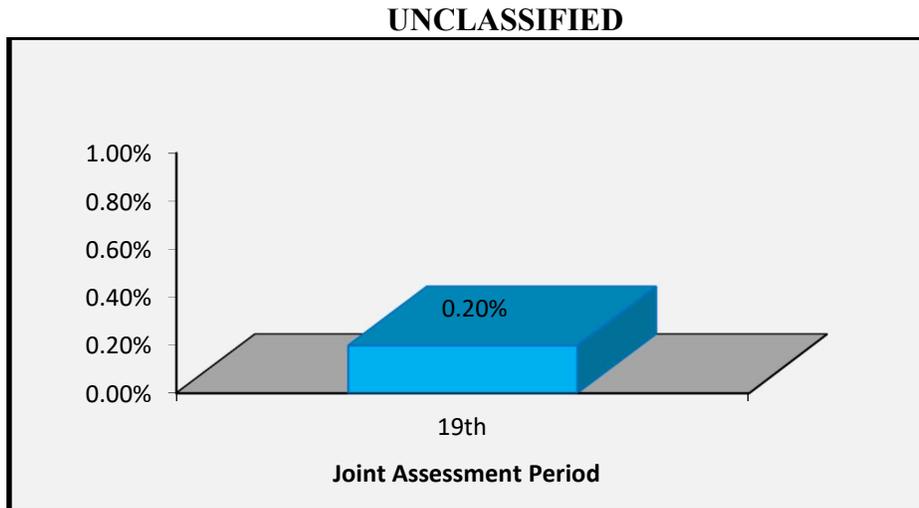
(U) Figure 15 is classified ~~TOP SECRET//SI//NOFORN~~.

(U) Similar to Figure 13 above and its associated explanation, the joint oversight team determined that excluding NSA’s notification delays incidents from the NSA’s Targeting Compliance Incident Rate provides a more valuable measure. Thus, Figure 16 shows that adjusted rate:

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN//FISA~~

(U) Figure 16: NSA Targeting Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), *not* including Notification Delays



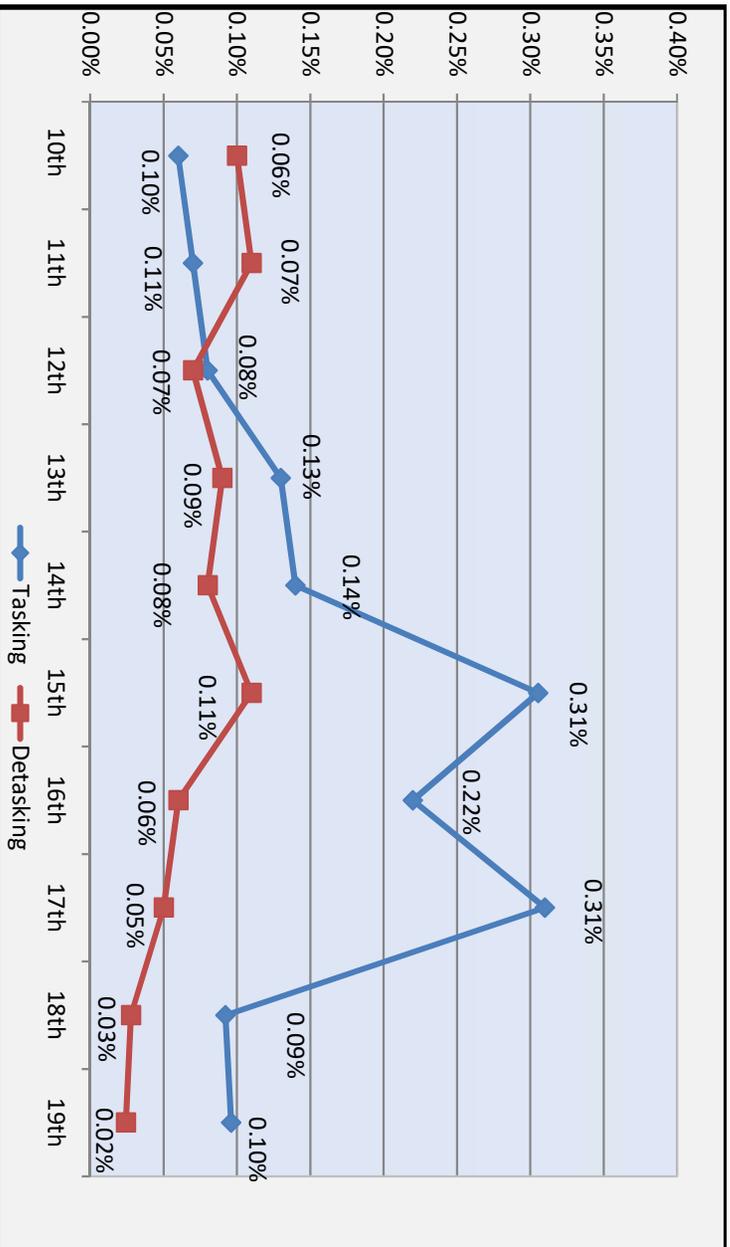
(U) Figure 16 is UNCLASSIFIED.

(U) Whereas Figure 16 depicts NSA targeting incidents by combining all targeting incidents, except for notification delays, Figure 17 depicts NSA's compliance incident rates individually for tasking and detasking incidents. Figure 17 separates those types of incidents for more granularity and understanding of the trends for each. As previously calculated and reported, the tasking and detasking incident rate is compared to the average facilities on collection for the given reporting period. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other, *i.e.* an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate.

~~TOP SECRET//SI//NOFORN//FISA~~

(U) Figure 17: NSA Tasking and Detasking Incident Compliance Rates

UNCLASSIFIED



(U) Figure 17 is UNCLASSIFIED.

(U) It is important to note that while Figure 17 provides a visual into trends of non-compliance, the non-compliance is less than 1%.⁴⁴ The tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection.⁴⁵

⁴⁴ (U) NSD and ODNI note that the above incident rates fluctuate by hundredths of a percentage point. Any perceived significant fluctuation is due to the scale of the graph (.00% to .25%). If, for example, the chart used a 0% to 1% scale to show fluctuations, the chart would show two virtually flat lines hugging the bottom. NSD and ODNI do not believe that the different incident rates are statistically significant and note that the incident rate is consistently quite low.

⁴⁵ (U) Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. Detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.

(U) As discussed in detail in the 15th Joint Assessment, the significant increase in tasking errors during that reporting period was substantially caused by one particular NSA targeting office's misunderstanding of the requirements of the targeting procedures. As a result, that particular targeting office was required to retake the formal NSA Section 702 online training. See the 15th Joint Assessment, pp. 35 – 36. As detailed in the 17th Joint Assessment,

~~TOP SECRET//SI//NOFORN/TISA~~

The tasking compliance incident rate involving facilities used by United States persons was almost zero. Detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.⁴⁶ The percentage of compliance incidents involving detasking incidents has remained consistently low. The detasking compliance incident rate involving facilities used by United States persons was almost zero.

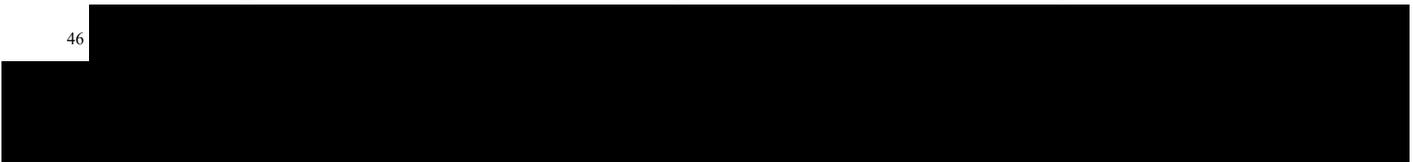
(U) C. FBI: Number of Compliance Incidents

(U) With respect to FBI's targeting procedures, the number of identified errors increased due to a significant increase in targeting errors caused by a software error in an FBI system that impacted multiple designated accounts and was subsequently corrected.⁴⁷ With respect to FBI's minimization procedures, the number of identified errors increased but remained relatively aligned to FBI's historically low number of such incidents.

(U) Classified Figure 18 shows the classified number of incidents for the last ten reporting periods (*i.e.*, from the 10th through the 19th reporting periods). With the exception of the 19th reporting period, the number of FBI's identified targeting and minimization errors remained consistently low. The joint oversight team assesses that FBI's overall compliance with its targeting and minimization procedures is a result of FBI's training and the processes it has designed to effectuate its procedures.

the increase in tasking errors during the 17th reporting period was not caused by a single targeting office's misunderstanding of the rules, but a number of the tasking errors consisted of a common fact pattern.

46



⁴⁷ ~~(S//NF)~~ Specifically,  incidents of noncompliance with the FBI targeting or minimization procedures were identified during this reporting period. Out of the total incidents,  were the result of a common issue in the application of FBI's targeting procedures (discussed later in this Joint Assessment).

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) Figure 18: Number of Compliance Incidents Involving the FBI Targeting and Minimization Procedures



(U) Figure 18 is classified ~~SECRET//NOFORN.~~

(U) D. CIA and NCTC: Number of Compliance Incidents

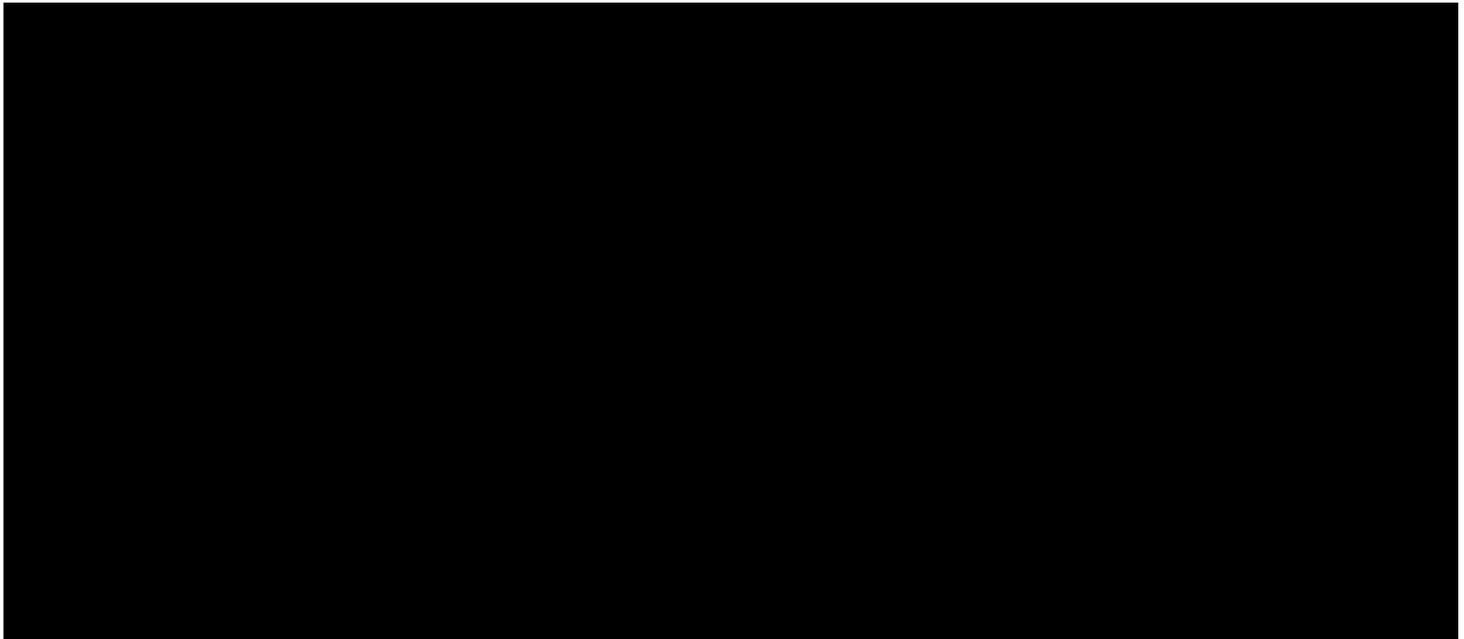
~~(S//NF)~~ There were [REDACTED] incidents during this reporting period that involved CIA's minimization procedures; [REDACTED] incidents were also reported in the previous reporting period for CIA. The joint oversight team assesses that CIA's compliance is a result of its training, systems, and processes that were implemented when the Section 702 program was developed to ensure compliance with its minimization procedures and the work of its internal oversight team.

~~(S//NF)~~ There was one⁴⁸ incident during this reporting period that involved NCTC's minimization procedures. The joint oversight team assesses that NCTC's compliance is a result of its training, systems, and process that were implemented when NCTC was authorized to receive certain unminimized Section 702-acquired information.

(U) Classified Figure 19 provides the classified number of minimization errors that involved CIA for the last ten reporting periods and NCTC for the current reporting period. These numbers have remained consistently low for CIA, and the number was low for NCTC for this reporting period. The joint oversight team assesses that CIA's and NCTC's compliance is a result of its training, systems, and processes that were implemented by each agency.

⁴⁸ (U) As noted above, on April 26, 2017, the FISC authorized NCTC to receive unminimized Section 702 data when it approved new Section 702 minimization procedures for NCTC (2016 NCTC Minimization Procedures). Thus, any minimization errors by NCTC would be included in the overall number of minimization errors only after April 26, 2017.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) Figure 19: Number of Compliance Incidents Involving the CIA or NCTC Minimization Procedures****(U) E. Service Providers: Number of Compliance Incidents**

~~(S//NF)~~ Finally, [REDACTED] incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents an increase from the zero incidents reported in the prior reporting period. The joint oversight team assesses that the low number of errors by the communications service providers is the result of continuous efforts by the Government and providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers' customers.

(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures

(U) As with the prior Joint Assessment, this Joint Assessment takes a broad approach and discusses the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The joint oversight team believes that analyzing the trends of those incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance. The Joint Assessment primarily focuses on incidents involving NSA's targeting and minimization procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA's targeting and minimization procedures. Most of those incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

compliance with NSA's minimization procedures involving the unintentional improper dissemination, retention, or querying of Section 702 information.

(U) Regardless of United States person status, robust oversight is conducted to ensure compliance with all aspects the targeting and minimization procedures; all identified incidents are reported to the Foreign Intelligence Surveillance Court (FISC) and to Congress; and all incidents are required to be appropriately remedied. For example, the joint oversight team identified compliance incidents where the non-United States person target was not reasonably expected to possess, receive, and/or likely communicate foreign intelligence information concerning a foreign power or foreign territory as defined in 50 U.S.C. § 1801(e). The accounts used by those users were detasked, the necessary purges were completed, including the recalling of disseminated reports if such reports were generated; and the relevant personnel were reminded of the Section 702 tasking requirements. As with all incidents, the joint oversight team works closely with NSA to identify causes of incidents in an effort to prevent future incidents, regardless of United States person status.

(U) The Section 707 Report provides further details regarding each individual incident and information on applicable remedial and mitigating actions. Details are provided as to how any erroneously acquired, disseminated, or queried information was handled through various purge, recall, and deletion processes. Information is also provided about personnel remediation and, when applicable, wider training efforts to address incidents. In certain instances, processes or technical tools are adjusted, as appropriate, to remedy the incidents, to mitigate impact, and to reduce the potential for future incidents.

(U) The NSA compliance incident rate for this reporting period, excluding FBI, CIA, and NCTC compliance incidents, is 0.33%⁴⁹ and represents a slight decrease from the compliance incident rate of 0.36% in the previous reporting period. In the subsections that follow,⁵⁰ this Joint Assessment examines some of the underlying causes of incidents of non-compliance focusing on incidents that have the greatest potential to impact United States persons' privacy interests, albeit that those incidents represent a minority of the overall incidents. This Joint Assessment first begins by examining and explaining incidents impacting United States persons' privacy interests, even though those incidents represent a minority of the overall incidents, followed by a discussion of other types of communication issues and human errors. The joint oversight team believes that analyzing the trends of these incidents, especially in regards to their causes, help the agencies focus resources, avoid future incidents, and improve overall compliance.

(U) A. The Impact of Compliance Incidents on United States Persons

(U) A primary concern of the joint assessment team is the impact of certain compliance incidents on United States persons. The Section 707 Report discusses every incident of noncompliance with the targeting and minimization procedures, including any necessary purges resulting from these incidents. Most of these incidents did not involve United States persons, and

⁴⁹ (U) The overall compliance incident rate for this reporting period is 0.42%.

⁵⁰ (U) Although ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may change with each joint assessment, depending on the incidents that occurred during that reporting period and the respective underlying causes.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

instead involved matters such as typographical errors in tasking that resulted in no collection, detasking delays with respect to facilities used by non-United States persons who had entered the United States, or notification errors.

(U) Some incidents, however, did involve United States persons during the recent reporting period. As noted above, both the tasking compliance incident rate and detasking compliance incident rate involving facilities used by United States persons was less than 0.01% during this reporting period. For tasking and detasking incidents, United States persons were primarily impacted by (1) tasking errors that led to the tasking of facilities used by United States persons, and (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person. United States persons were also impacted by minimization errors during this reporting period, which are detailed below. While the number of incidents involving United States persons remains low, due to their importance, these incidents are highlighted in this subsection. The Section 707 Report provides further details regarding each individual incident and how any erroneously acquired, disseminated, or queried United States person information was handled through various purge, recall, and deletion processes.

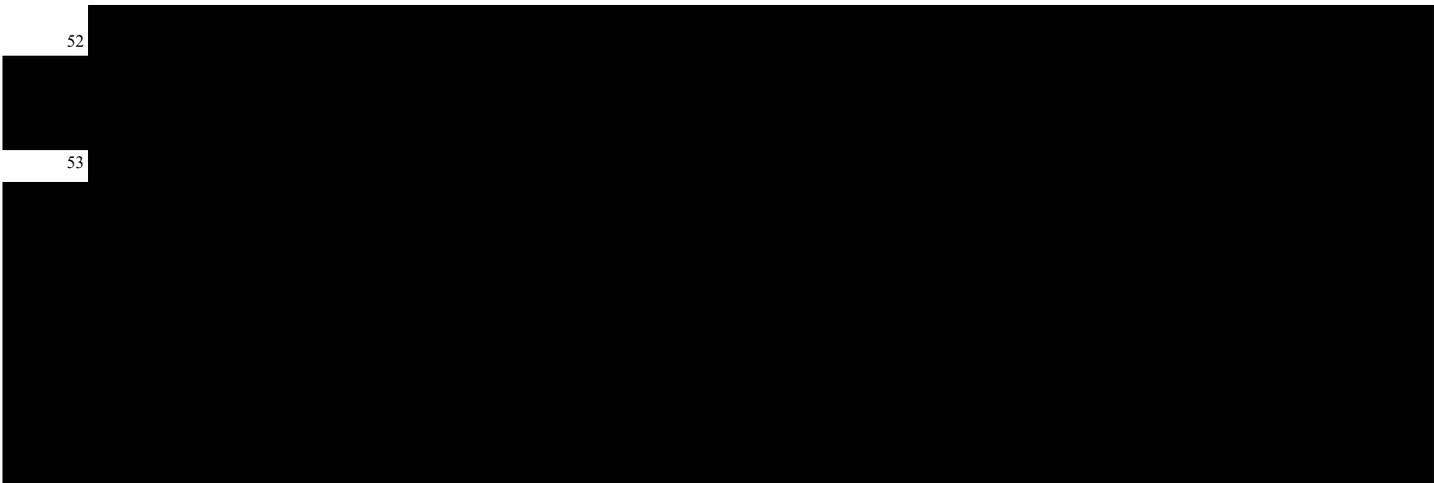
(U) (1) Tasking Errors Impacting United States Persons

(U) Only 2% of the total number of tasking errors identified during this reporting period involved instances where facilities used by United States persons were tasked pursuant to Section 702.⁵¹ These incidents represent isolated instances of insufficient due diligence and did not involve an intentional effort to target a United States person.

(U) All of the tasking errors in this reporting period impacting United States persons involved the tasking of facilities where the Government knew or should have known that at least one user of the facility was a United States person.⁵² The majority of these tasking errors involved typographical errors made by targeting analysts when submitting the facilities to be tasked pursuant to Section 702.⁵³ The remaining tasking errors involved targeting analysts not considering the

⁵¹ (U) Note that this is 2% of all tasking incidents. As described above, the overall tasking compliance incident rate involving United States persons was less than 0.002%.

52



53

~~TOP SECRET//SI//NOFORN/FISA~~

totality of circumstances known to the Government prior to targeting pursuant to Section 702.⁵⁴ In these incidents, personnel were reminded of the Section 702 tasking requirement, any applicable collection was deleted, and no reporting was identified based on the collection.

(U) (2) Delays in Detasking Impacting United States Persons

(U) The majority of the detasking incidents involved (i) non-United States persons who either traveled to the United States or appeared to have traveled to the United States or (ii) an unexplained indication of an account that appeared to have been accessed from within the United States. Only 9.6% of the total number of detasking delays involved facilities used by a United States person.⁵⁵ As discussed in further detail below, the detasking delay incidents impacting United States persons in this reporting period were caused by human errors (*i.e.*, misunderstandings of the detasking requirements and analysts' faulty analysis of information that erroneously led them to continue to assess that the target was a non-United States person located outside the United States). In these incidents, the relevant personnel were reminded of the Section 702 detasking requirements. If information was acquired, it was deleted; if reporting based on the erroneous collection was identified, it was recalled. Information that was identified as not being appropriately deleted or recalled would be reported as a compliance incident.

~~(TS//SI//NF//FISA)~~ Of the detasking delays involving facilities used by United States persons,⁵⁶ incidents involved a misunderstanding of the detasking requirements. For example,

[REDACTED]

[REDACTED] the relevant NSA personnel were reminded of the detasking requirements. [REDACTED]

⁵⁴

[REDACTED]

⁵⁵ (U) Note that this is 9.6% of all detasking incidents. As described above, the overall detasking compliance incident rate involving United States persons was less than 0.002%.

⁵⁶

[REDACTED]

⁵⁷

⁵⁸

~~TOP SECRET//SI//NOFORN/FISA~~

~~(TS//SI//NF)~~ Other incidents were the result of faulty analysis that led to delays in detasking facilities used by United States persons.⁶⁰ For example,

(U) B. Effect of Human Error

(U) (1) Errors That Can Be Addressed Through Training

(U) Unlike in the immediately prior section, which focused exclusively on incidents impacting United States persons, this section addresses incidents that impacted both United States persons and non-United States persons. As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established processes to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated. For example, despite multiple pre-tasking checks, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors accounted for approximately 13% of the tasking errors made in this reporting period, which is a slight increase from the previous reporting period, in which typographical errors accounted for 11% of the tasking errors.⁶¹ Approximately 21% of the detasking delays from this reporting period were the result of inadvertent errors, such as an NSA analyst detasking some, but not all, of a target's facilities that required detasking.⁶² As with other compliance incidents, any data acquired as a result of such tasking and detasking errors is required to be purged.

59

60

61

62

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) Other types of errors can also be addressed and alleviated through training – in particular, certain types of tasking errors related to conducting necessary pre-tasking checks to establish “foreignness” (*i.e.*, that the user is a non-United States person located outside the United States). Approximately 50% of the tasking errors in this reporting period (an increase from 40% in the last reporting period) involved instances in which NSA did not take sufficient pre-tasking steps to try to find information regarding the location of the targeted user or otherwise did not properly establish a sufficient basis to assess that the targeted user was located outside the United States. The two most common examples include situations in which the analyst did not conduct a necessary pre-tasking check or there was too long of a delay between the necessary pre-tasking checks and the actual tasking of the account.⁶³ In all of these incidents, NSA advised that there is no indication that these facilities were used by a United States person or by someone in the United States.

(U) After discussing these incidents with NSA compliance personnel, NSA took remedial steps. NSA compliance personnel advised that they have met in person with target offices to reiterate the FAA 702 targeting guidance regarding foreignness checks. NSA also held training in 2017 for Section 702 adjudicators who review proposed taskings, and during that training, NSA reminded them of the need to conduct the relevant foreignness checks prior to tasking and to ensure that the checks are done within seven days of approving a tasking. NSA continued to post guidance on this issue on several NSA internal webpages to reach as wide an audience as possible. In addition, and new to this reporting period, NSA worked with the developers responsible for NSA’s tasking tool to determine whether a technical solution to these types of errors was feasible; an effort that has continued past this current reporting period. To date, NSA identified numerous challenges to implementing a technical solution, which rendered those solutions infeasible. Even without new technical solutions, the joint oversight team assesses that these types of tasking errors are preventable and recommends that NSA continue to reinforce this issue with analysts and adjudicators as part of regular training. Notably, the joint oversight team’s review of compliance incidents *subsequent* to this reporting period has revealed a significant decrease in these types of incidents, thus demonstrating the impact from the above non-technical steps taken by NSA.

(U) Other tasking errors related to establishing a valid “foreign intelligence information purpose” (*i.e.*, that the target user is reasonably expected to possess, receive, and/or likely communicate foreign intelligence information as defined in 50 U.S.C. § 1801(e)). Specifically, in approximately 15% of tasking errors, (an increase from the previous reporting period)⁶⁴ NSA did not have a sufficient basis to assess that the user of the tasked facility would be reasonably expected to possess, receive, or likely communicate foreign intelligence information related to a specific group listed in Exhibit F of a particular certification.⁶⁵ In those instances, at the time of tasking,

63



⁶⁴ (U) The number of this type of tasking errors was so few in the last reporting period that they were not discussed in the previous joint assessment. However, those incidents were reported in the Attorney General’s Section 707 Report.

65

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

NSA had sufficiently established that the users were non-United States persons located outside the United States.⁶⁶ Although NSA intended to acquire foreign intelligence information related to a specific Exhibit F group, NSD and ODNI concluded there was not a reasonable basis to assess that the user of the facility possessed, was expected to receive, and/or was likely to communicate foreign intelligence information concerning a foreign power or foreign territory listed on Exhibit F in effect during this time period. NSA detasked the facilities and purged any collection and recalled any reporting as required by its minimization procedures.

~~(S//NF)~~ In addition to the types of tasking errors discussed above, human error also resulted in documentation errors, which increased to approximately 23.6% of the total number of compliance incidents in this period from 14% in the prior reporting period.⁶⁷ The NSA targeting procedures require that for each tasked facility, NSA document the source of the “foreignness determination” (*i.e.*, information showing that the user of that facility was reasonably believed to be located outside the United States) and identify the foreign power or foreign territory about which NSA expects to obtain foreign intelligence information. The targeting procedures also require a written explanation of the basis for NSA’s assessment at the time of targeting that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked (“foreign intelligence purpose”). In all of these incidents, while the actual tasking of each facility was appropriate, the analyst failed to sufficiently document the “foreignness determination” or the “foreign intelligence information purpose” on the tasking sheet. As in the past, NSD discussed these errors with NSA compliance personnel and has sought information from NSA on the cause of the increase and measures NSA can take to reduce such errors.

(U) Finally, there were a number of reported incidents where NSA properly followed all of its procedures, but failed to timely provide the required notice to NSD and ODNI when a tasked selector was used from within the United States or by a United States person. These notification errors increased to 22% in this reporting period from 11% in the last reporting period.⁶⁸ Many of

⁶⁶ (U) NSA ultimately determined that two of the tasked facilities were used by a United States person and promptly detasked those facilities. The joint oversight team assesses that NSA’s tasking of these facilities was not in error with respect to its foreignness determinations and assessments of non-U.S. person status of the users at the time of tasking.

⁶⁷

⁶⁸

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

these notification errors resulted from a training issue involving one employee, whereas numerous other notification errors were caused by one NSA office.⁶⁹ NSA has addressed the miscommunication in training with the individuals involved and will also ensure that reporting procedures are clearly conveyed to compliance personnel in the future. In addition, NSA is developing a more routine auditing process to ensure that any notification mistakes due to human error are identified in an expeditious manner

(U) (2) Minimization Errors: Prevention Through Training and Technical Improvements

(U) NSA's minimization procedures have various requirements, including rules regarding *querying* raw Section 702-acquired information, rules regarding under what circumstances Section 702-acquired information may be *disseminated*, and rules regarding how long raw Section 702-acquired information may be *retained*. Whenever possible, all erroneous query results were deleted, disseminated reports were recalled, and collection purged. Relevant personnel were reminded of the Section 702 query, dissemination, and retention requirements, as appropriate. Particular issues of non-compliance with minimization procedures are detailed below.

(U) Querying Rules. During this reporting period, NSA's minimization procedures included two types of restrictions on querying raw Section 702 collection.

- 1) NSA's Section 702 minimization procedures require that queries of raw Section 702 collection *must be designed in a manner "reasonably likely to return foreign intelligence information."* For example, if a query is determined to be overly broad under this standard (*e.g.*, typographical or comparable error in the construction of the query term),⁷⁰ it constituted a compliance incident, regardless of whether the query term used a non-United States person identifier or a United States person identifier.
- 2) Although NSA's Section 702 minimization procedures permit queries of raw Section 702 collection using United States person identifiers, such queries *must be approved in accordance with NSA's internal procedures*. If an NSA analyst used a United States person identifier that had not been approved pursuant to NSA's internal procedures to query Section 702-acquired data, it constituted a compliance incident.

⁶⁹ (U) The notification errors caused by the one employee accounted for approximately 24% of all notification errors (*i.e.*, 5% of all compliance incidents by NSA). The notification errors caused by different employees in one NSA office (NSA OCO) accounted for approximately 21% of all notification errors (*i.e.*, 4.6% of all compliance incidents by NSA).

⁷⁰ (U) These overly broad query errors are typically traceable to a typographical or comparable error in the construction for the query. For example, an overly broad query can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overly broad results as a result of the query.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) The previous Joint Assessment discussed a third restriction (pertaining to queries in upstream collection); however, NSA's updated Section 702 minimization procedures in effect for this reporting period no longer contain that restriction.

(U) Specifically, in April 2017, NSA ceased collecting "abouts" communications in Section 702 "upstream" internet surveillance. Instead, NSA limited such collection to internet communications that are sent directly to or from a foreign target.⁷¹ In May 2017, ODNI publicly explained that, in response to NSA's action, the Government amended the 2016 Certifications in March 2017, to include submitting to the FISC amended Section 702 targeting and minimization procedures for NSA that authorize only the acquisition of communications to or from a Section 702 target.⁷² Because of the more restricted nature of NSA's reconfigured upstream Internet collection, certain restrictions in the use of U.S. person identifiers to query Internet communications acquired through NSA's Section 702 upstream collection have been removed.⁷³ In considering the 2016 Certifications, as amended in March 2017, the FISC determined that the changes NSA made to its upstream Internet collection sufficiently addressed the compliance incidents involving the inadvertent use of U.S. person identifiers as query terms.⁷⁴ The FISC ultimately determined that NSA's targeting and minimization procedures, as amended, were consistent with FISA and the Fourth Amendment to the Constitution.⁷⁵

(U) Compared with the previous reporting period, the overall minimization incident rate decreased to 17% from the 40% in the previous reporting period.⁷⁶ As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization procedures. During this reporting period, out of all of NSA's total minimization errors, approximately 76.6% involved improper queries,⁷⁷ of which:

- approximately 28% of the minimization errors involved overly broad queries.⁷⁸

⁷¹ (U) See NSA's public statement, dated April 28, 2017, "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702" at <https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activities.shtml>.

⁷² (U) See ODNI's website *IC on the Record* on May 11, 2017.

⁷³ (U) See FISC's April 2017 Opinion at 23-30.

⁷⁴ (U) See *id.* at 29.

⁷⁵ (U) See *id.* at 95.

⁷⁶ [REDACTED]

⁷⁷ (U) In the previous reporting period, approximately 92.4% of NSA's minimization procedures errors involved improper queries.

⁷⁸ [REDACTED]

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

- approximately 48% involved NSA analysts conducting queries using a United States person identifier without approval as required by NSA's internal procedures.⁷⁹

As in previous reporting periods, there were no NSA incidents of an analyst intentionally running improper queries.

(U) One example of an overly broad query incident involved an analyst entering a parenthesis in the wrong place in the query, as well as a misunderstanding of the requirement to obtain pre-approval prior to querying United States person identifiers. Another example of a query incident involved an analyst who conducted a United States person query in Section 702 collection, but, due to a misunderstanding, failed to obtain pre-approval for the query. When an NSA analyst conducts an improper U.S. person query or overly broad query, NSA reminds the relevant personnel of the query requirements.

(U) Dissemination rules. In addition to querying rules, NSA's minimization procedures also set forth requirements for the dissemination of United States person information. In the current reporting period, incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in NSA's minimization procedures represented approximately 16% of the total number of minimization incidents (compared to 5% of minimization incidents during the last reporting period). As was the case with NSA querying incidents, there were no identified NSA incidents of an analyst intentionally violating the dissemination rules.

(U) In one example, NSA issued a report that included the names of United States persons whose identities were not necessary to understand foreign intelligence information.⁸⁰ The error occurred because the person responsible for releasing the report mistakenly issued the report without realizing that the analyst who had drafted the report had not yet minimized and masked the United States person identities. NSA recalled the report. In another example, NSA discovered that an NSA analyst had issued a report that contained information from which United States persons' identities could be ascertained and whose identities were not necessary to understand foreign intelligence information.⁸¹ The error occurred because the analyst had identified the United States persons in general terms without specific identifying information and believed that doing so was adequate. However, from context, the United States person identities could be ascertained. NSA recalled the report and reissued it without the contextual identification of United States persons. In all of the incidents involving improper disseminations, NSA reminded the relevant personnel of the dissemination requirements.

79

80

81

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) C. Inter-Agency and Intra-Agency Communications**

(U) Section 702 compliance requires good communication and coordination within and between agencies. In order to ensure targeting decisions are made based on the totality of the circumstances and after the exercise of due diligence, those involved in the targeting decision must communicate the relevant facts to each other. Analysts also must have access to the necessary records that inform such decisions. Good communication among analysts is needed to ensure that facilities are promptly detasked when it is determined that the Government has lost its reasonable basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Furthermore, query rules regarding United States person identifiers and dissemination decisions regarding United States person information require inter- and intra-agency communications regarding who the Government has determined to be a United States person.

(U) In this reporting period, approximately 27% of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.⁸² This is an increase from last reporting period's 13% and, thus, the joint oversight team assesses the need for improvement in communicating. The detasking delays caused by miscommunication typically involved travel or possible travel of non-United States persons to the United States, and none of these incidents resulted in the delayed detasking of a facility used by a United States person. Significantly, however, less than 1% of all tasking errors involved situations in which intra-agency miscommunications resulted in the erroneous tasking of a facility.⁸³

(U) The joint oversight team assesses that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its on-going oversight efforts, the joint oversight team will also continue to monitor NSA, CIA, and FBI's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

(U) III. Review of Compliance Incidents – FBI Targeting and Minimization Procedures

(U) There was a significant increase in the number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period.⁸⁴ However, 87% of the targeting incidents were related to the same type of error that was caused by a technical software issue that has since been addressed.⁸⁵ These tasking incidents involved no collection that would

82

83

84

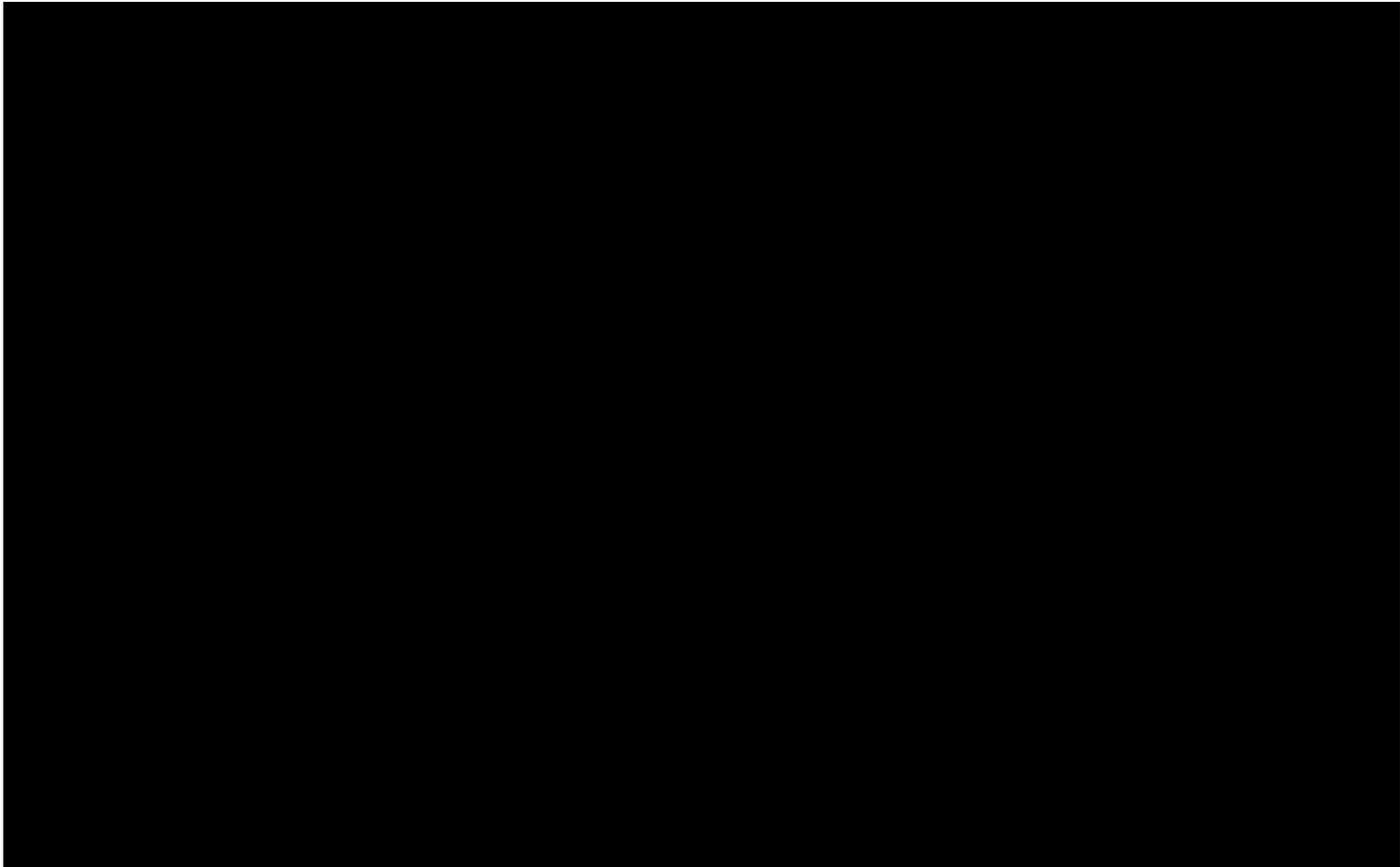
85

~~TOP SECRET//SI//NOFORN/FISA~~

have been unauthorized had the technical issue not occurred. Many of the minimization incidents were caused by employees misunderstanding the query requirements in the minimization procedures. Of note, during this reporting period, the joint oversight team determined that there were two minimization incidents that involved intentional violations of the minimization procedures. Both incidents are discussed in detail below.

(U) A. Targeting Incidents

~~(S//NF)~~ As noted above, [REDACTED] incidents involving non-compliance with FBI's targeting procedures were caused by a technical issue that has since been addressed. Specifically,



[REDACTED] FBI advised that it has implemented safeguards to prevent these types of errors from occurring in the future.

⁸⁶ [REDACTED]

⁸⁷ ~~(S//NF)~~ Section I.4 of FBI's Section 702 targeting procedures provides: "In the ordinary course of determining whether t [REDACTED]"

~~TOP SECRET//SI//NOFORN/FISA~~**(U) B. Minimization Incidents – Retention Errors Caused by Misunderstanding**

(U) During this reporting period, most of FBI's minimization incidents involved improper queries, which are detailed below. However, there were also some incidents that involved non-compliance with the other requirements of the FBI minimization procedures, including the provisions concerning establishment of a review team for a target charged with a crime pursuant to United States Code. Specifically, as soon as the FBI knows that a target is charged with such a crime, FBI's minimization procedures require that the FBI follow certain steps, including establishing a review team of monitor(s). The member(s) of the review team must be individuals who have no role in the prosecution, and the monitor(s) initially review the Section-702 acquired information to determine whether the communications are privileged. Failure to timely establish such a review team constitutes a compliance incident.

~~(S//NF)~~ Specifically, [REDACTED] involved the failure to timely establish such a review team.⁸⁸ The joint oversight team assesses that these types of incidents typically are the result of individual failures or confusion. Given the reduction of these incidents over successive reporting periods, the joint oversight team assesses that NSD's oversight reviews, NSD's and FBI's training at FBI field offices on the attorney-client privileged communication provisions of the minimization procedures, and the [REDACTED] tool FBI uses [REDACTED] will help facilitate both the identification of review team compliance incidents and assist in the prevention of any future incidents. In fact, the review team incident identified during this reporting period was discovered as a result of FBI's [REDACTED] tool. The joint oversight team assesses that continued oversight and training, as well as FBI's [REDACTED] tool, will continue to help facilitate both the identification of review team compliance incidents and assist in the prevention of any future incidents.

~~(S//NF)~~ The remaining FBI incidents involved minor violations of aspects of the Section 702 minimization procedures.⁸⁹ For example, [REDACTED] involved FBI's storage of raw FISA-acquired information in a system that does not comply with the minimization procedures, [REDACTED]. The government addressed this matter through revisions to the FBI's Section 702 minimization procedures.

(U) C. Minimization Incidents - Query Errors Caused by Misunderstanding or Lack of Awareness

(U) During this reporting period, most of the improper queries resulted from FBI personnel misunderstanding the querying rules even though the queries were conducted for work-related purposes. These queries were not, however, reasonably likely to return foreign intelligence information or evidence of a crime and, thus, constituted incidents. In most of the instances, FBI personnel did not fully understand the query standard. In some instances, FBI personnel were unable to recall why they conducted certain queries. In other incidents, FBI personnel were generally unaware of, or were not thinking of, the fact that their queries would be running against

88

89

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

raw FISA-acquired information and did not intend to return such information. In the incidents below, FBI personnel were reminded of the rules regarding queries.

~~(S//NF)~~ Specifically, [REDACTED] FBI incidents involved FBI personnel conducting non-compliant queries in an FBI system containing raw FISA-acquired information, including Section 702-acquired information.⁹⁰ In one incident, an analyst queried his/her own name to find a product he/she had marked in the system. In another, at the request of an agent, an analyst queried the agent's name and date of birth to find the agent's passport number in an FBI system that also contained raw Section 702-acquired information.

(U) D. Minimization Incidents - Query Errors Caused by Possible Intentional Action

(U) While the majority of noncompliant query incidents were inadvertent errors often resulting from misunderstanding the rules, there were two unique incidents that were not inadvertent. The first incident involved FBI personnel conducting certain categorical batch queries (as opposed to queries conducted on the basis of individualized assessments) during a period of time when FBI's Office of General Counsel sought NSD's legal view on whether the queries could be conducted under the applicable query standard. At the time the queries were conducted, the relevant FBI personnel had been instructed not to conduct the queries as the legal issue was being considered. "Categorical batch queries" include any query that relies on a categorical justification for multiple query terms associated with more than one person, and, hence, for which there is no individualized assessment for each of the identifiers queried. The second intentional incident involved a FBI personnel who NSD had previously counseled about conducting improper queries and who subsequently continued to conduct improper queries.

~~(S//NF)~~ Specifically, in the first incident, FBI's [REDACTED] conducted batch queries using identifiers for over 70,000 facilities associated with anyone who had access to FBI building facilities or systems, including both FBI and non-FBI employees.⁹¹ The batch queries ran against an FBI database that includes unminimized Section 702-acquired information. The oversight team concluded that those queries, although performed as [REDACTED] lawfully authorized function [REDACTED] were inconsistent with FBI's minimization procedures because the batch queries were not reasonably likely to return foreign intelligence information. Prior to running these queries, [REDACTED] had sought guidance from FBI's Office of General Counsel (OGC) regarding whether those batch queries would be permitted by the FBI's minimization procedures. FBI OGC in turn raised this question with NSD and advised [REDACTED] no such queries should be conducted until and unless approval was granted by NSD and OGC. At the time the above queries were conducted, the legal question was still being considered, and neither NSD nor OGC had cleared those queries to be conducted. [REDACTED] had been instructed to not run the queries until the legal consideration was completed, [REDACTED] run the queries. [REDACTED]

90

91

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

who authorized these queries to be conducted was reminded that the queries should not have been run until approved by NSD and OGC.

(U)

~~(U//FOUO)~~ The second query incident that appeared to be intentional involved one individual FBI worker. During an oversight review at a FBI field office in 2017, NSD discovered that this individual conducted improper United States person queries using the individual's own name and that of another FBI personnel that were not compliant with the query restrictions in FBI's minimization procedures.⁹² Unlike other improper queries by FBI personnel who misunderstood the rules and conducted queries of United States persons for work-related purposes, this individual worker conducted queries that did not appear to be work-related. Furthermore, this same individual had previously conducted improper queries on multiple occasions using what appeared to be United States person identifiers and had been previously reminded of the minimization rules.⁹³ After discovering that this was not the individual's first time conducting improper queries of a similar nature, the matter was referred to FBI's Security Division. The individual was subsequently removed from the FBI, and the individual's security clearance was revoked.

(U) **VI. Review of Compliance Incidents – CIA Minimization Procedures**

~~(U)~~ During this reporting period, there were [REDACTED] incidents involving noncompliance with the CIA minimization procedures. Those incidents involved inadvertent instances of CIA not completely removing Section 702-acquired information that should have been deleted from CIA systems.

~~(S//NF)~~ Specifically, [REDACTED] involved the inadvertent failure to purge and age off a portion of unminimized Section 702-acquired data due to technical issues.⁹⁴ CIA has updated its

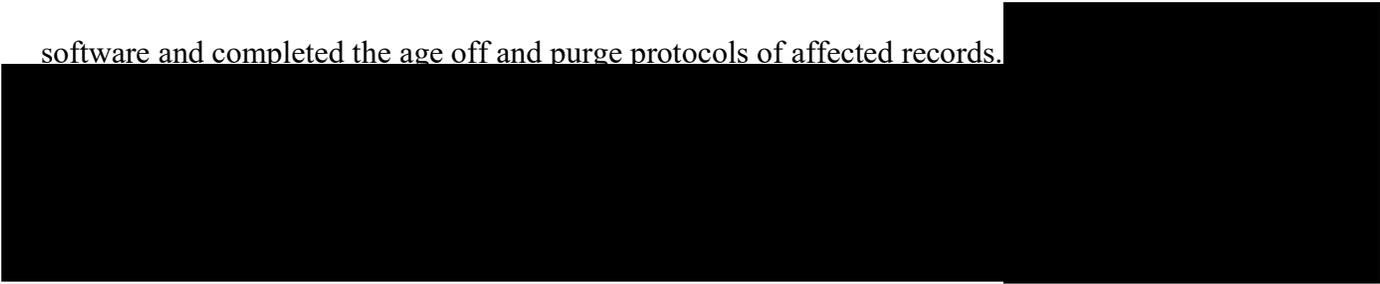
92

93

94

~~TOP SECRET//SI//NOFORN/FISA~~

software and completed the age off and purge protocols of affected records.



(U) V. Review of Compliance Incidents – NCTC Minimization Procedures

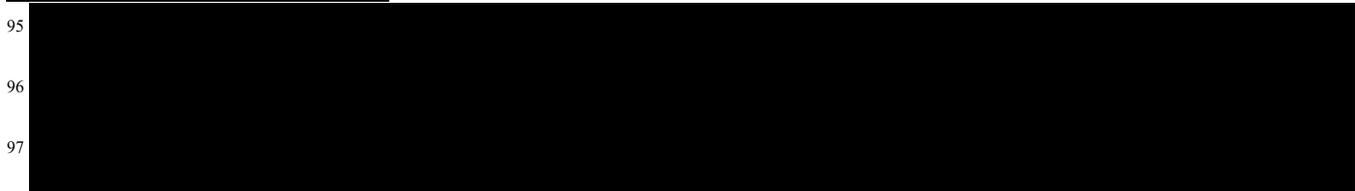
(U) During the reporting period, there was one incident involving a violation of NCTC’s minimization procedures. In that incident, an NCTC analyst conducted an overly broad query that was not reasonably likely to identify foreign intelligence information.⁹⁶ To address this issue, NCTC issued guidance in November 2017, reminding all system users to include limiting terms and qualifiers when designing queries to find and extract foreign intelligence information.

(U) VI. Review of Compliance Incidents – Provider Errors

~~(S//NF)~~ During this reporting period, [redacted] instances of noncompliance (compared to no incidents during the last reporting period) by an electronic communication service provider with a Section 702(h) directive, [redacted] which affected numerous facilities.⁹⁷



A hearing was held by the FISC regarding this matter. This incident has been the subject of multiple notices regarding remediation efforts [redacted] to address this compliance issue. [redacted] employ both technical and human checks to identify, prevent, and/or mitigate such overproduction incidents, these protections did not identify [redacted] overproduction in this instance. Given that errors by the service providers can result in the acquisition of United States person information, the joint oversight team assesses that the agencies must continue to diligently monitor the acquisitions that the providers transmit to the Government. Agencies must also continue to work with the service providers to prevent future incidents of non-compliance.



95
96
97

(U)⁹⁸ ~~(U//FOUO)~~ This matter was the subject of a Congressional notification by NSA to the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence. In addition, in December 2017, at HPSCI’s request, the government provided a briefing on this matter for HPSCI staff members.

~~TOP SECRET//SI//NOFORN/FISA~~**(U) SECTION 5: CONCLUSION**

(U) During this reporting period, the joint oversight team found that the agencies continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. Although the number of compliance incidents continued to remain small, particularly when compared with the total amount of collection activity, a continued focus is needed to address the underlying causes of the incidents that did occur. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection activities and continued personnel training. Additionally, as part of its on-going oversight responsibilities, the joint oversight team and the agencies' internal oversight regimes will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

APPENDIX

~~TOP SECRET//SI//NOFORN/FISA~~

APPENDIX

(U) IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

(U) I. Overview - NSA

(U) The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).¹ As required by Section 702, those targets must be non-United States persons² reasonably believed to be located outside the United States.

~~(S//NF)~~ During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:



¹ (U) Specifically, Section 701(b)(4) provides:

The term ‘electronic communication service provider’ means – (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

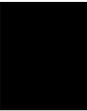
² (U) Section 101(i) of FISA defines “United States person” as follows:

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

3



4



~~TOP SECRET//SI//NOFORN/FISA~~

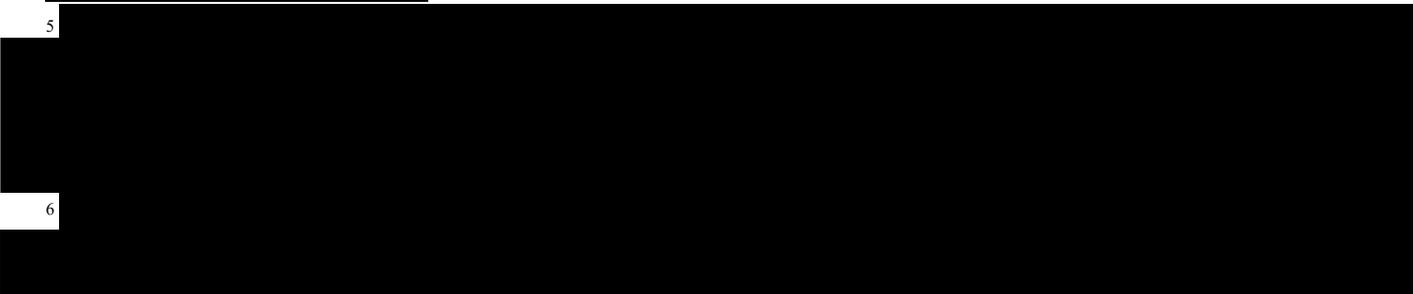
(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to receive or communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General's Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

(U) Under NSA's FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a "selector") is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.⁵ In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA "tasks" that facility in the relevant tasking system. The facilities are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

(U) After information is collected from those tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA, FBI, and NCTC, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA, FBI, and NCTC in accordance with their respective FISC-approved Section 702 minimization procedures.⁶

(U) NSA's targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably

5



6

~~TOP SECRET//SI//NOFORN/FISA~~

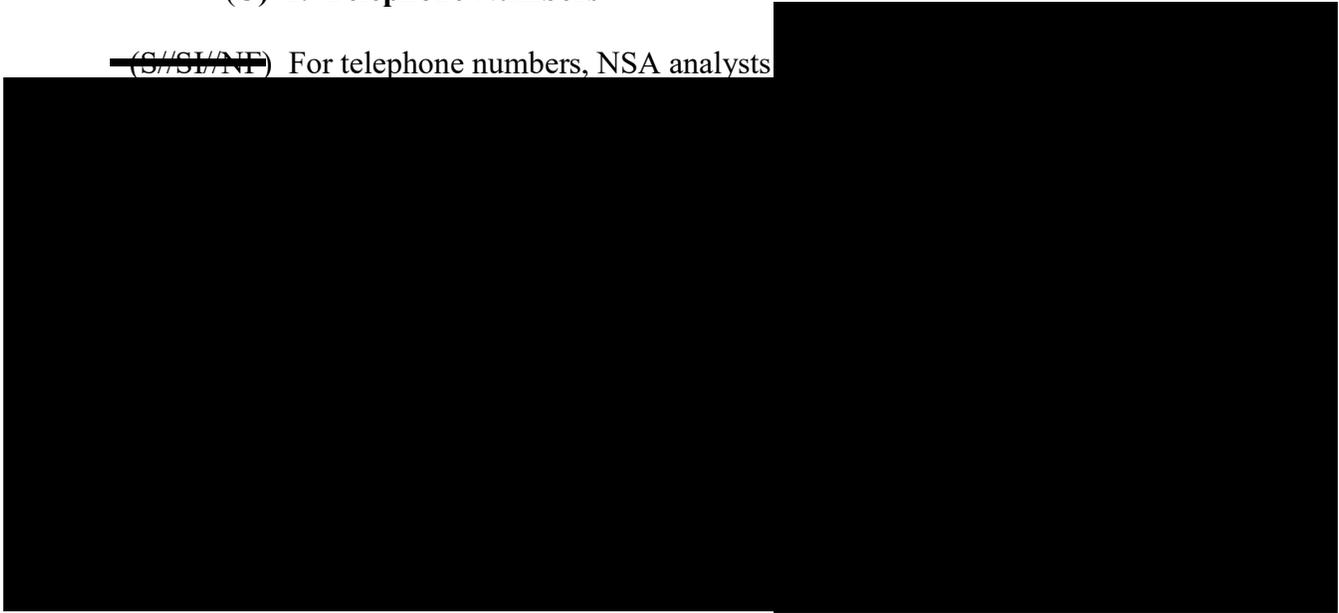
~~TOP SECRET//SI//NOFORN/FISA~~

believed to be located outside the United States, the post-targeting analysis conducted on the facilities, and the documentation required.

(U) A. Pre-Tasking Location

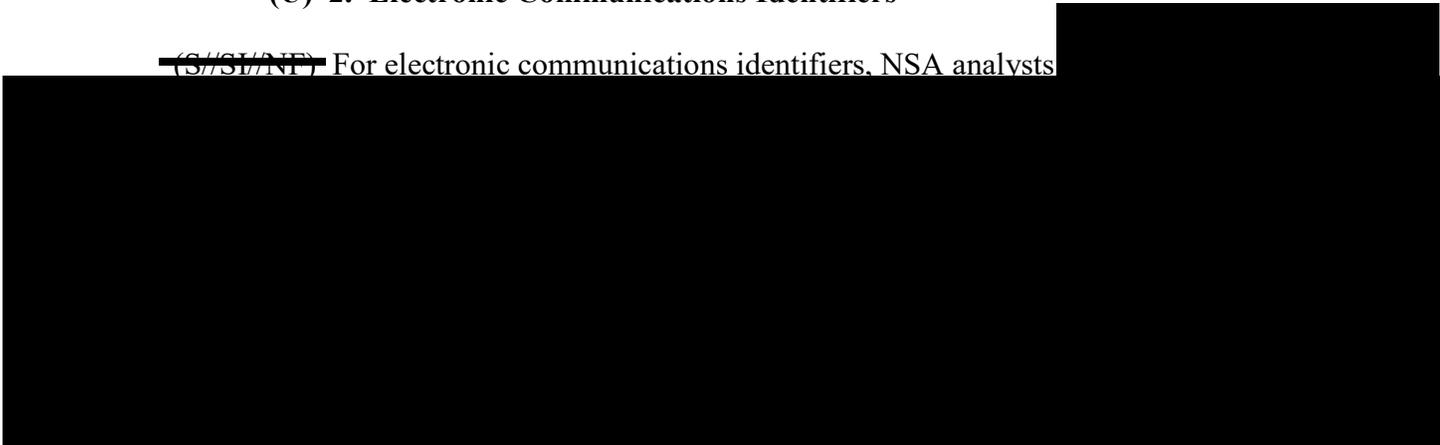
(U) 1. Telephone Numbers

~~(S//SI//NF)~~ For telephone numbers, NSA analysts



(U) 2. Electronic Communications Identifiers

~~(S//SI//NF)~~ For electronic communications identifiers, NSA analysts

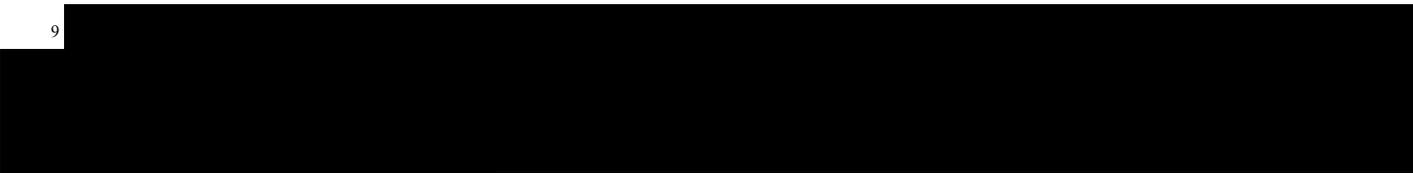


7



⁸ (U) Analysts also check this system as part of the “post-targeting” analysis described below.

9



~~TOP SECRET//SI//NOFORN/FISA~~

(U) B. Pre-Tasking Determination of United States Person Status



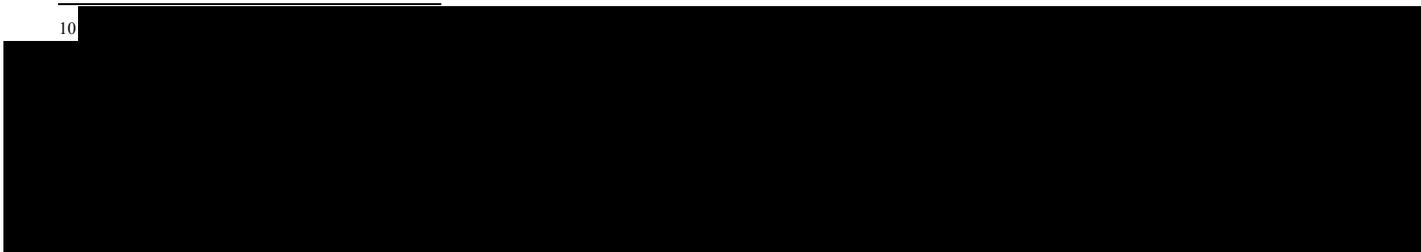
(U) C. Post-Tasking Checks



~~(S//REL TO USA, FVEY)~~ NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA's review of [redacted] a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority [redacted]

Should traffic not be viewed at least once every 30 business days, a

¹⁰



¹¹ ~~(S//NF)~~ NSA's automated notification system to ensure analysts have reviewed collection is currently implemented only for [redacted], not [redacted]. NSA is attempting to develop a similar system for [redacted]

~~TOP SECRET//SI//NOFORN/FISA~~

notice is sent to the tasking team and their management, who then have the responsibility to follow up.

(U) D. Documentation

~~(S//NF)~~ The procedures provide that analysts will document in the tasking database a citation to the information leading them to reasonably believe that a targeted person is located outside the United States. The citation is a reference that includes the source of the information, [REDACTED] enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable belief. Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information.

~~(S//NF)~~ NSA has [REDACTED] an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. [REDACTED] to assist analysts as they conduct their work. This tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain fields and features for targeting, documentation, and oversight purposes. Accordingly, the tool allows analysts to document the required citation to NSA records on which NSA relied to form the reasonable belief that the target was located outside the United States. [REDACTED]

[REDACTED] The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields [REDACTED] each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

(U) NSA's targeting procedures also require analysts to identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information and provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory.

(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked. The joint oversight team assesses that the TAR has improved the oversight team's ability to understand NSA's foreign intelligence purpose in tasking facilities.

~~(S//NF)~~ [REDACTED]
[REDACTED]. Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the record or records relied upon by the analyst, [REDACTED] the analyst's foreignness explanation, the targeting rationale, [REDACTED] These records,

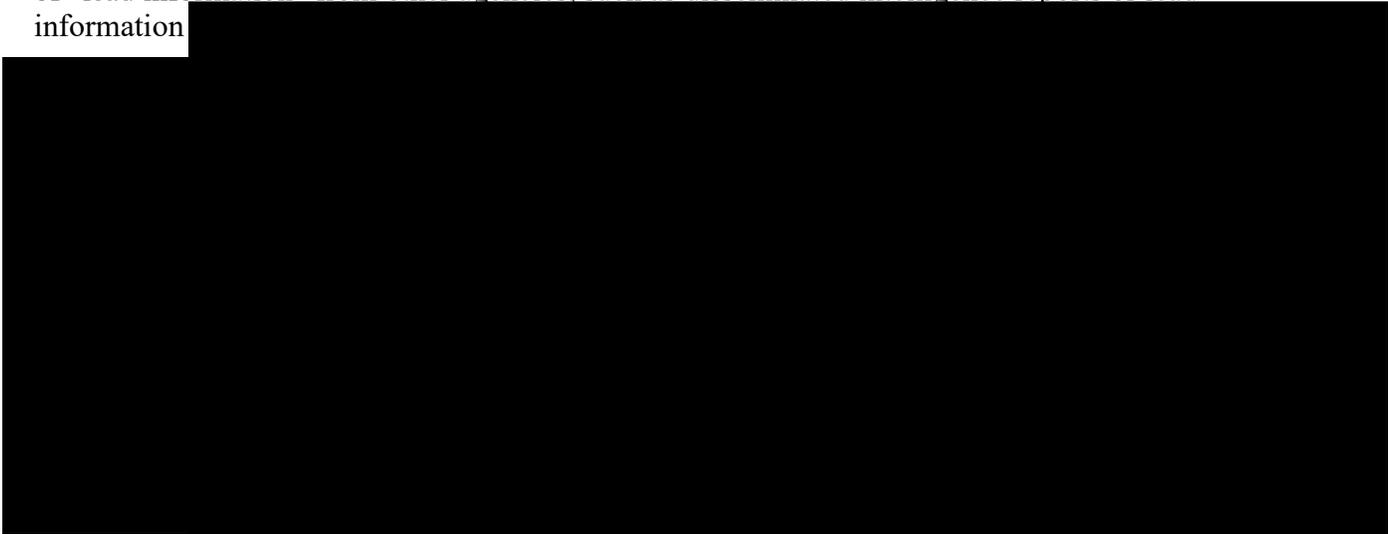
A-6

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

referred to as “tasking sheets,” are reviewed by the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

~~(S//NF)~~ The source records cited on these tasking sheets are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations recorded on the tasking sheets. Other source records may consist of “lead information” from other agencies, such as disseminated intelligence reports or lead information



(U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA OGC and OCO training program; review the targeting and minimization procedures as well as other documents filed with the certifications; and must pass a competency test. The databases NSA analysts use are subject to audit and review by OCO. For guidance, analysts consult standard operating procedures, supervisors, OCO personnel, and NSA OGC attorneys.

(U) The NSA targeting and minimization procedures also require NSA to conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA Office of the Inspector General (NSA OIG) and NSA OGC. NSA’s OCO reviews all Section 702 taskings and conducts spots checks of disseminations based in whole or in part on Section 702-acquired information. The Directorate of Operations Information and Intelligence Analysis organization also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

(U) NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. Compliance officers work with NSA analysts and CIA and FBI points of contact, as necessary, to compile incident reports that are forwarded to both the NSA OGC and OIG. NSA OGC forwards the incidents to NSD and ODNI.

A-7

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

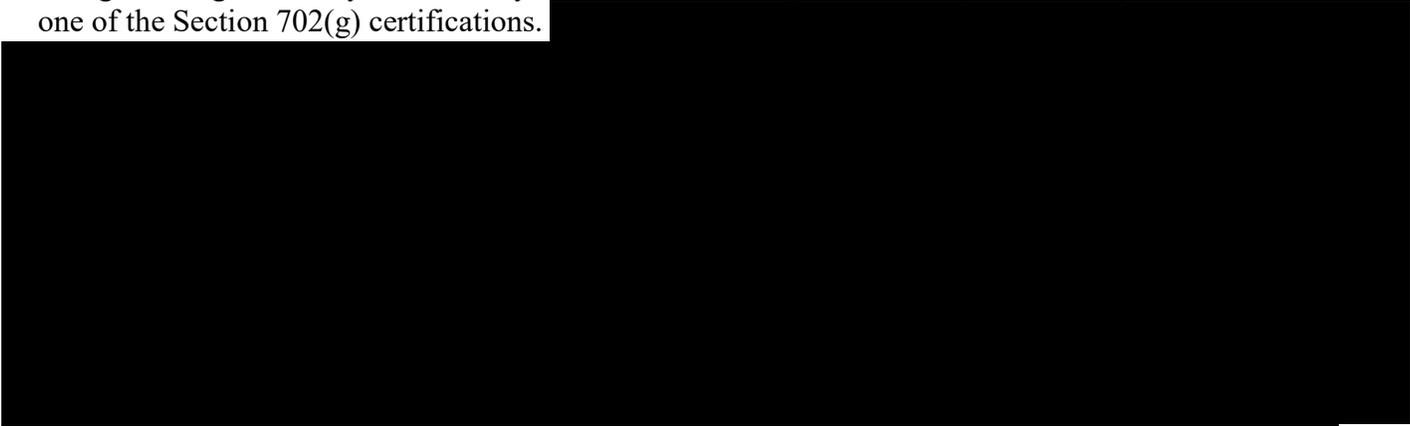
(U) On a more programmatic level, under the guidance and direction of the Compliance Group, NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protections during NSA missions. The Compliance Group complements and reinforces the intelligence oversight program of the NSA OIG and oversight responsibilities of NSA OGC.

(U) A key component of the CMCP is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort, known as “Rules Management,” focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA and (2) technological solutions to support (and simplify) Rules Management activities. The Authorities Integration Group coordinates NSA’s use of the Verification of Accuracy (VoA) process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy and compliance officials within NSA. NSA has also developed a Verification of Interpretation (VoI) review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA’s FISA activities. The Compliance Group has developed a risk assessment process to assess the potential risk of non-compliance with the rules designed to protect United States person privacy. The assessment is conducted and reported to the NSA Deputy Director and NSA Senior Leadership Team biannually.

(U) II. Overview - CIA

(U) A. CIA’s Role in Targeting

~~(S//NF)~~ Although CIA does not target or acquire communications pursuant to Section 702, CIA has put in place a process, in consultation with NSA, FBI, NSD, and ODNI, to identify foreign intelligence targets to NSA (hereinafter referred to as the “CIA nomination process”). Based on its foreign intelligence analysis, CIA may “nominate” a facility to NSA for potential acquisition under one of the Section 702(g) certifications.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~~~(S//NF)~~

Nominations are reviewed and approved by a targeting officer's first line manager, a component legal officer, a senior operational manager and the FISA Program Office prior to export to NSA for tasking.

~~(S//NF)~~ The FISA Program Office was established in December 2010

and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts. The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

(U) B. Oversight and Compliance

(U) CIA's FISA compliance program is managed by its FISA Program Office in coordination with CIA OGC. CIA provides small group training to personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination and minimization questions. Identified incidents of noncompliance with the CIA minimization procedures are generally reported to NSD and ODNI by CIA OGC.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) III. Overview NCTC**

~~(S//NF)~~ NCTC does not target or acquire communications pursuant to Section 702. In addition, NCTC does not currently have a process in place to identify or nominate foreign intelligence targets to NSA. However, like CIA and FBI, NCTC may request to be ~~redacted~~ on unminimized data (pertaining to counterterrorism) from Section 702 facilities already tasked by NSA. NCTC applies its Section 702 minimization procedures to Section 702 ~~redacted~~ data.

~~(S//NF)~~ NCTC, in consultation with NSD, developed an electronic and data storage system, known as ~~redacted~~ to retain and process raw FBI-collected FISA-acquired information in accordance with NCTC's Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act. In consultation with NSD, ODNI, NSA, and FBI, NCTC modified ~~redacted~~ to (i) provide additional compliance capabilities in support of ~~redacted~~ FISA Section 702-acquired counterterrorism data and (ii) monitor compliance with NCTC's Minimization Procedures for Section 702-acquired counterterrorism data (Section 702 minimization procedures). In addition to documenting compliance with the Section 702 minimization procedures requirements, ~~redacted~~ also documents the requests for ~~redacted~~ Section 702-acquired information. This documentation includes th ~~redacted~~

~~(S//NF)~~ ~~redacted~~ communications from Section 702 tasked facilities are stored within ~~redacted~~ where only properly trained and authorized analysts are able to query them.

~~(S//NF)~~ NCTC personnel may disseminate Section 702-acquired information of or concerning an unconsenting United States person if that information meets the standard for dissemination pursuant to Section D of NCTC's Section 702 Minimization Procedures.

~~(S//NF)~~ ~~redacted~~ NCTC's Compliance and Transparency Group (hereafter NCTC Compliance) within the Office of Data Strategy and Innovation conducts periodic reviews of Section 702 ~~redacted~~ as well as NCTC Section 702 disseminations in order to verify compliance with NCTC's Section 702 Minimization Procedures and identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) B. Oversight and Compliance**

(U) NCTC's FISA compliance program is managed by NCTC Compliance in coordination with NCTC Legal. NCTC provides training to all NCTC personnel who may access raw FISA-acquired information. Access to unminimized Section 702-acquired communications is limited to trained personnel. NCTC compliance personnel and attorneys also respond to inquiries regarding minimization questions. Identified incidents of noncompliance with the NCTC Section 702 Minimization Procedures are reported to NSD and ODNI generally by NCTC Compliance or NCTC Legal personnel.

~~(S//NF)~~ ^(U) NCTC Compliance was established in the fall of 2014 and is charged with providing strategic direction for the management and oversight of NCTC's access to and use of all datasets pursuant to executive order, statute, interagency agreement, applicable IC policy, and internal policy. This includes management and oversight of NCTC's FISA programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA, FBI, and CIA. In addition, the office leads the day-to-day FISA compliance efforts within NCTC. NCTC Compliance is responsible for providing strategic direction and internal oversight for data handling and management of FISA/Section 702 data, as well as administering and implementing NCTC FISA/Section 702 training, ensuring that all NCTC Section 702 collection is properly [REDACTED] minimized and disseminated, and that NCTC is complying with all minimization procedures requirements.

(U) IV. Overview - FBI**~~(U)~~ A. FBI's Role in Targeting – Nomination for Acquiring [REDACTED] Communications**

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition of [REDACTED] communications. [REDACTED]

A- 11

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

[REDACTED] including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to [REDACTED]

[REDACTED] The FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate [REDACTED] FBI must then apply its own, additional procedures, which require FBI to review NSA's conclusion of foreignness [REDACTED]

— ~~(S//NF)~~ More specifically, after FBI obtains the tasking sheet from NSA, it reviews the information provided by NSA regarding the location of the person and the non-United States person status of the person. [REDACTED]

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

[REDACTED]

~~(S//NF)~~ Unless FBI locates information indicating that the user is a United States person or is located inside the United States [REDACTED]

[REDACTED]

~~(S//NF)~~ If FBI identifies information indicating that NSA's determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve [REDACTED]

[REDACTED]

(U) C. Documentation

~~(S//NF)~~ The targeting procedures require that FBI retain the information [REDACTED] in accordance with its records retention policies [REDACTED]. [REDACTED] FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [REDACTED] extending through [REDACTED] and culminating in approval or disapproval of the acquisition. In addition, the FBI standard operating procedures call for [REDACTED] depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications [REDACTED] regarding its review of the [REDACTED] information. Additional checklists have been created to capture information on requests withdrawn [REDACTED] or not approved by FBI.

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

(U) D. Implementation, Oversight, and Compliance

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI OGC, particularly the National Security and Cyber Law Branch (NSCLB), as well as the Electronic Communications Surveillance Unit's (ECSU) Technology and Data Innovation Section (TDI, formerly named the Exploitation Threat Section (XTS)), [REDACTED] and Inspection Division (INSD) [REDACTED]

[REDACTED] TDI has the lead responsibility in FBI for [REDACTED] requests [REDACTED] TDI personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests for [REDACTED] [REDACTED] TDI also has the lead responsibility for facilitating FBI's nominations to NSA [REDACTED] communications. TDI, NSLB, NSD, and ODNI have all worked on training FBI personnel to ensure that FBI nominations and post-tasking review comply with the NSA targeting procedures. Numerous such trainings were provided during the current reporting period. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in the FBI's [REDACTED]

[REDACTED] In addition, NSD conducts training on the Section 702 minimization procedures at multiple FBI field offices each year.

(U) ~~(S//NF)~~ The FBI's targeting procedures require periodic reviews by NSD and ODNI at least once every 60 days. FBI must also report incidents of non-compliance with the FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. TDI and NSCLB are the lead FBI elements in ensuring that NSD and ODNI received all appropriate information with regard to these two requirements.

(U) V. Overview - Minimization

(U) After a facility has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, CIA and NCTC. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

(U) Section 702 minimization procedures do, however, impose additional obligations or restrictions as compared with the minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located

A- 14

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

(U) NSA, CIA, NCTC, and FBI have created systems to track the purging of information from their systems. CIA, NCTC, and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.

~~TOP SECRET//SI//NOFORN/FISA~~